

Summit Switch Installation and User Guide

Extreme Networks, Inc.

10460 Bandley Drive

Cupertino, California 95014

(888) 257-3000

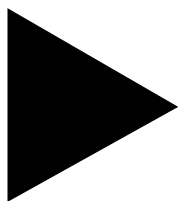
<http://www.extremenetworks.com>

Published September 1997

Copyright © **Extreme Networks, Inc., 1997**. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without permission from Extreme Networks, Inc.

Extreme Networks, ExtremeWare, Summit, and the Extreme Networks logo are trademarks of Extreme Networks.

All other brand and product names are registered trademarks or trademarks of their respective holders.



PREFACE

This preface provides an overview of this guide, describes guide conventions, tells you where to look for specific information and lists other publications that may be useful.

INTRODUCTION

This guide provides the required information to install and configure the Summit1 and Summit2 Gigabit Ethernet Switch.

This guide is intended for use by network administrators who are responsible for installing and setting up network equipment. It assumes a basic working knowledge of

- Local Area Networks (LANs)
- Ethernet concepts
- Ethernet switching and bridging concepts
- Simple Network Management Protocol (SNMP)



If the information in the Release Notes shipped with your Switch differs from the information in this guide, follow the Release Notes.

TERMINOLOGY

When features, functionality, or operation is specific to a particular model of the Summit family, the model name is used (for example, Summit1 or Summit2).

Explanations about features and operations that are the same among all members of the Summit family simply refer to the product as the Summit.

CONVENTIONS

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1: Notice Icons




Icon	Notice Type	Alerts you to...
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.

Table 2: Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names appear in text in one of two ways: <ul style="list-style-type: none">■ Referred to by their labels, such as “the Return key” or “the Escape key”■ Written with brackets, such as [Return] or [Esc] If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].
Words in <i>italicized</i> type	Italics emphasize a point or denote new terms at the place where they are defined in the text.
Words in boldface type	Bold text denotes key features.

The command syntax is explained in [Chapter 4](#).

RELATED PUBLICATIONS

The Summit documentation set includes the following:

- Summit Quick Reference Guide
- Summit Release Note

You may find the following Web site of interest:

- Extreme Networks Home Page: <http://www.extremenetworks.com/>

1

Summit Overview

This chapter describes the following:

- Summit1 and Summit2 features
- How to use the Summit family of switches in your network configuration
- Summit front views
- Summit rear view
- Factory default settings

ABOUT THE SUMMIT FAMILY OF SWITCHES

Network managers are currently faced with the challenge of creating networks that can provide ultra-fast speed and high performance to serve the needs of today's network users, while simultaneously preserving the investment they have made in Ethernet and Fast Ethernet technology.

By addressing the entire spectrum of Ethernet data rates (10/100/1000 Mbps), the Summit family of LAN switches enables you to introduce high-speed Gigabit Ethernet backbones into your existing network, while maintaining established connections to the 10 Mbps and 100 Mbps segments that already exist.

SUMMARY OF FEATURES

The Summit family of switches is comprised of two models: the Summit1 and the Summit2.

Both switches have the following features:

- Support for 128K addresses in the Switch forwarding database
- Fully nonblocking operation
 - All ports transmit and receive packets at wire speed
- Autonegotiation for half- or full-duplex operation
- Optional redundant power supply
- Redundant physical Gigabit Ethernet backbone connection
- Virtual local area networks (VLANs) including support for 802.1Q
- Quality of Service (QoS)
- Spanning Tree Protocol (STP) (IEEE 802.1D) with multiple STP domains
- Wirespeed Internet Protocol (IP) routing via Routing Information Protocol (RIP) version 1 and RIP version 2
- Integrated network management
- Console connection
- Telnet connection
- Web interface
- Simple Network Management Protocol (SNMP) support

PORT CONNECTIONS

The Summit1 provides eight Gigabit Ethernet ports. Six of the ports are fixed 1000Base-SX ports using 850nm duplex SC connectors. Two of the ports are modular, and support the standard Gigabit Interface Connector (GBIC). This enables you to select various types of fiber and copper modules to support longer distances or lower cost. The Summit1 can be ordered with either two 1000Base-SX or two 1000Base-LX GBIC transceivers already installed. GBIC transceivers can also be ordered separately.

Figure 1-1 shows the front view of the Summit1.

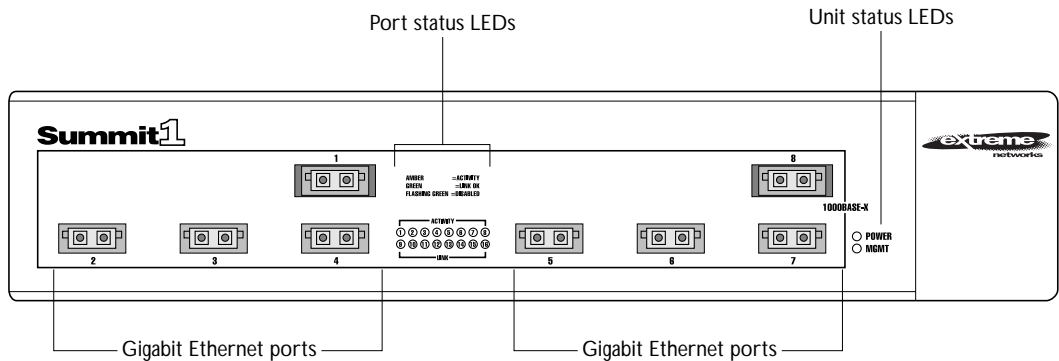


Figure 1-1: Summit1 front view

The Summit2 is a workgroup switch featuring sixteen 10Base-T/100Base-TX ports, two Gigabit Ethernet uplinks, and one redundant Gigabit Ethernet uplink. The 10Base-T/100Base-TX ports use standard RJ-45 connectors. They are autosensing for 10/100 Mbps operation, as well as half- or full-duplex operation. The Gigabit Ethernet interfaces support the GBIC connector, and ship with standard 1000Base-SX, 850nm GBIC modules. Additional cable types are also supported.

Figure 1-2 shows the front view of the Summit2

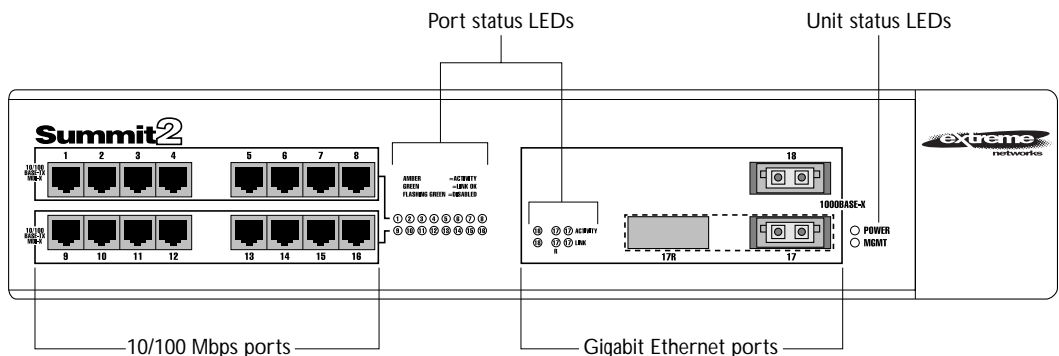


Figure 1-2: Summit2 front view

FULL-DUPLEX

The Summit Switch provides full-duplex support for all ports. Full-duplex allows frames to be transmitted and received simultaneously and, in effect, doubles the bandwidth available on a link. All 10/100 Mbps ports on the Summit autonegotiate for half- or full-duplex operation.

PORT REDUNDANCY

The Summit2 has an optional redundant Gigabit Ethernet port. Using the redundant port, you can dual-home the Summit2 to one or two Switches. [Figure 1-3](#) illustrates a Summit2 dual-homed to two different Switches.

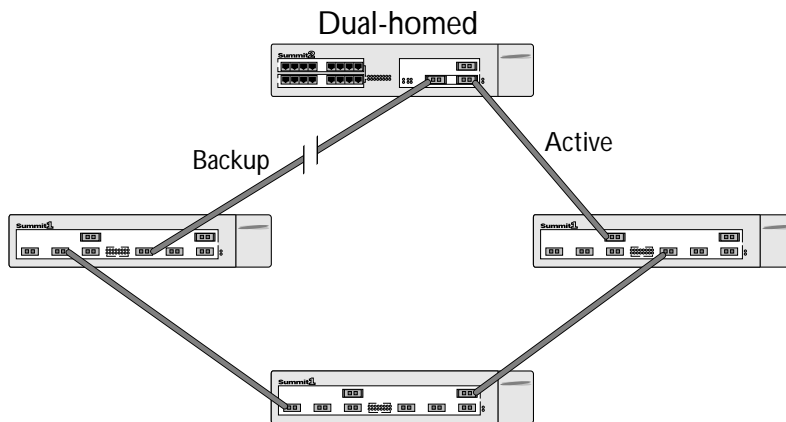


Figure 1-3: Dual-homing configuration

In the event that the active port fails or loses link status, the redundant port is automatically activated. When the primary port resumes operation, the redundant port becomes inactive. The redundant port cannot be used for load sharing.

VIRTUAL LANs (VLANs)

The Summit has a VLAN feature that enables you to construct your broadcast domains without being restricted by physical connections. Up to 255 VLANs can be defined on the Summit. A VLAN is a group of location- and topology-independent devices that communicate as if they were on the same physical local area network (LAN). Implementing VLANs on your network has the following three advantages:

- It helps to control broadcast traffic. If a device in VLAN *marketing* transmits a broadcast frame, only VLAN *marketing* devices receive the frame.
- It provides extra security. Devices in VLAN *marketing* can only communicate with devices on VLAN *sales* using a device that provides routing services.
- It eases the change and movement of devices on networks. If a device in VLAN *marketing* is moved to a port in another part of the network, all you must do is specify that the new port belongs to VLAN *marketing*.



For more information on VLANs, refer to [Chapter 5](#).

SPANNING TREE PROTOCOL (STP)

The Summit supports the IEEE 802.1D Spanning Tree Protocol (STP), which is a bridge-based mechanism for providing fault tolerance on networks. STP enables you to implement parallel paths for network traffic, and ensure the following:

- Redundant paths are disabled when the main paths are operational.
- Redundant paths are enabled if the main traffic paths fail.

The Summit supports up to 64 Spanning Tree Domains (STPDs).



For more information on STP, refer to [Chapter 7](#).

QUALITY OF SERVICE (QoS)

The Summit has Quality of Service (QoS) features that enable you to specify service levels for different traffic groups. By default, all traffic is assigned with the “normal” QoS profile. If needed, you can configure some traffic to have different guaranteed minimum bandwidth, maximum bandwidth, and priority.



For more information on Quality of Service, refer to [Chapter 8](#).

IP UNICAST ROUTING

The Summit can route IP traffic between the VLANs that are configured as virtual router interfaces. Both dynamic and static IP routes are maintained in the routing table. RIP version 1 and RIP version 2 are supported.



For more information on IP unicast routing, see [Chapter 9](#).

NETWORK CONFIGURATION EXAMPLES

This section describes where to position the Summit1 and Summit2 within your network.

One common use of the Summit is on a Gigabit Ethernet backbone. [Figure 1-4](#) shows an example of a Gigabit Ethernet backbone within a building.

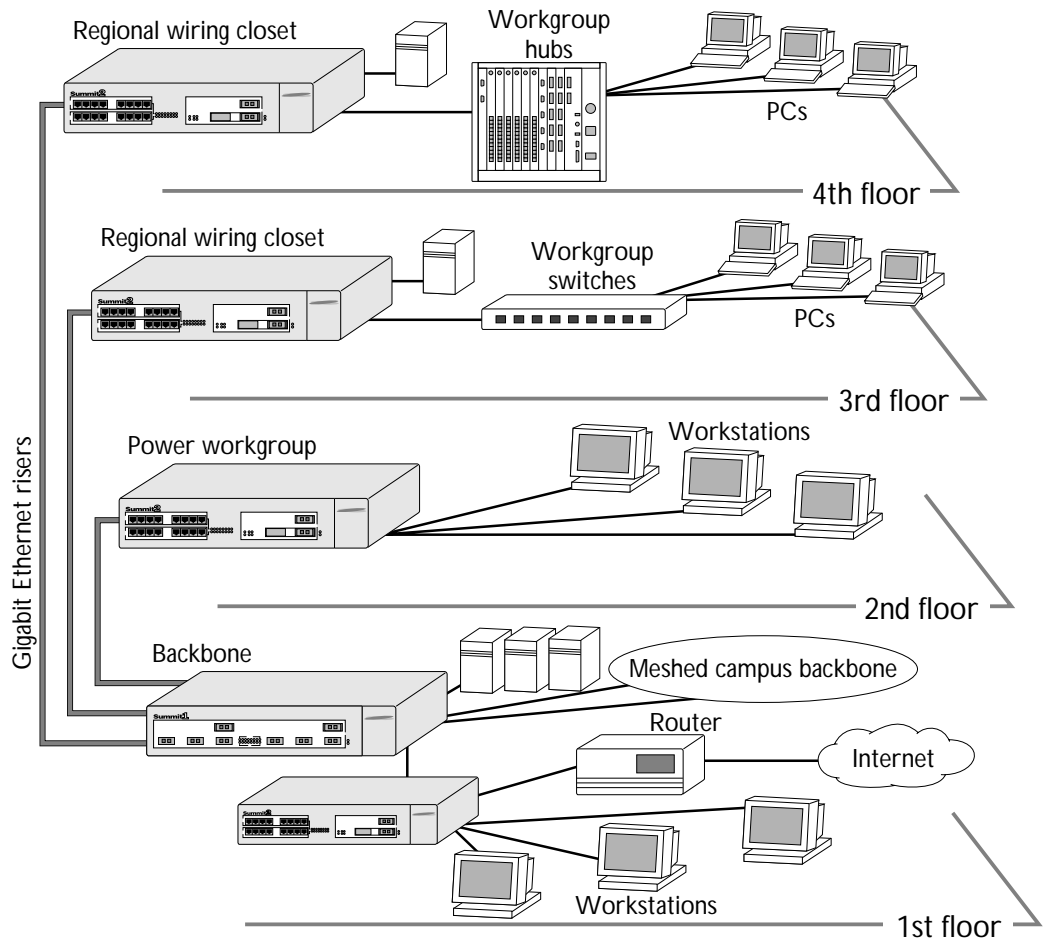


Figure 1-4: Summit family used in a backbone configuration

The Summit2 on each floor is connected to the backbone Summit1 using a 1 Gbps, full-duplex link. Using Gigabit Ethernet as a backbone technology removes bottlenecks by providing scalable bandwidth, low-latency, high-speed data switching.

As well as providing a fast-switched backbone between Ethernet LANs, Gigabit Ethernet-equipped file servers and devices may be directly attached to the Summit1, providing improved performance to the Ethernet desktop.

Another common use for the Summit family is in a campus environment, as shown in [Figure 1-5](#).

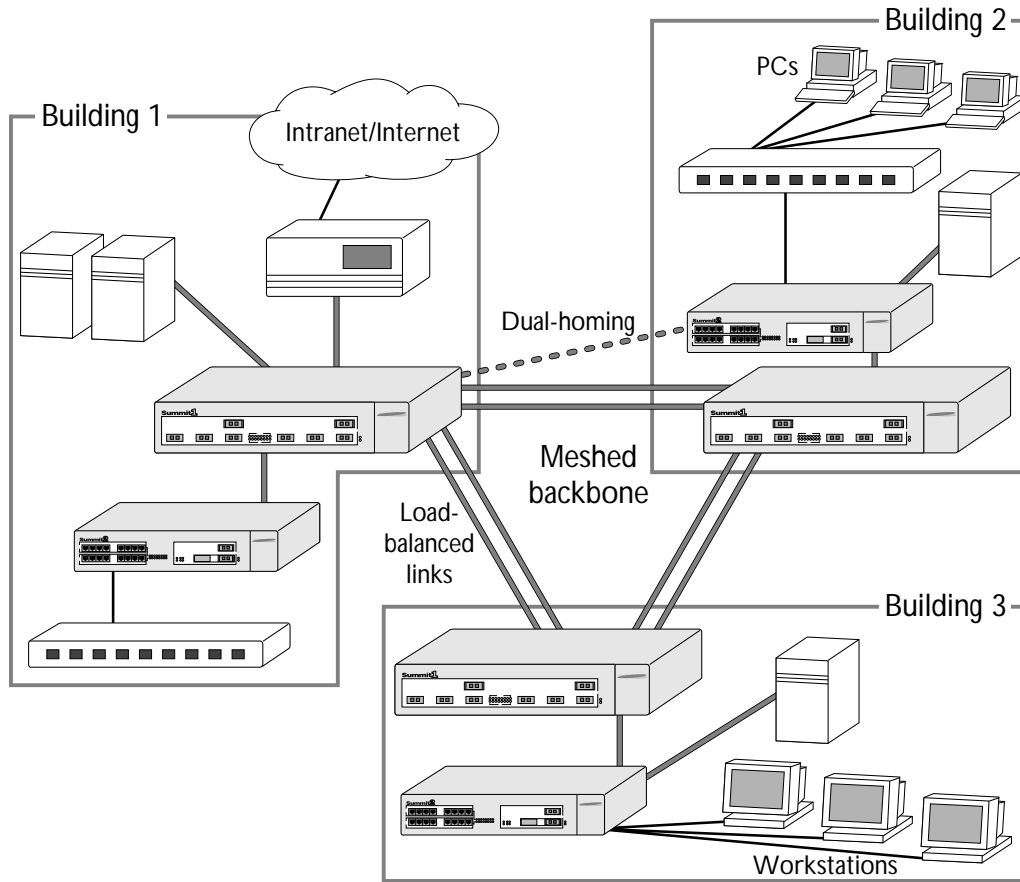


Figure 1-5: Summit family used in a campus environment

The Summit1 switches located in each building form a meshed backbone, providing load balancing and redundancy. In addition, the Summit2 Switch in Building 2 is dual-homed to the Summit1 located in Building 1 and to the Summit1 located in Building 3.

SUMMIT1 FRONT VIEW

Figure 1-6 shows the Summit1 front view.

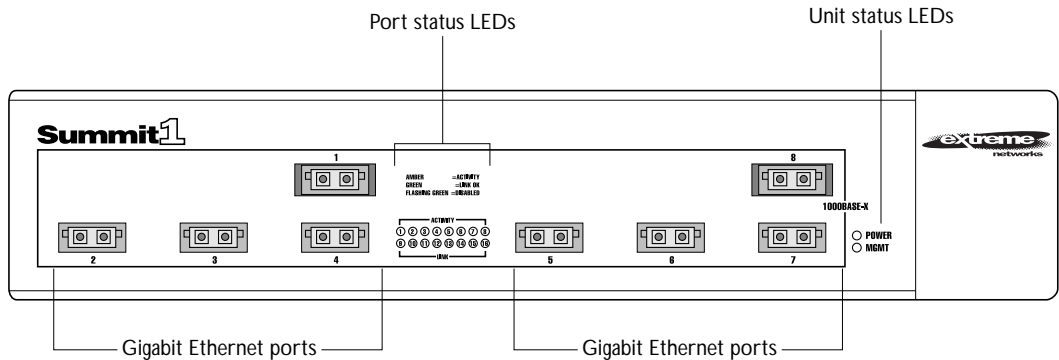


Figure 1-6: Summit1 front view

PORTS

The Summit1 has eight Gigabit Ethernet ports. Six of the ports use SC connectors and support 1000Base-SX over 850nm fiber-optic cable. Ports 1 and 8 have GBIC connectors and support the media types and distances listed in [Table 1-1](#).

Table 1-1: Summit1 Supported Media Distances for GBIC Connectors

Gigabyte Type	Distance		
	50/125 micro Multimode Fiber	62.5/125 micron Multimode Fiber	Single-mode Fiber
850nm Multimode Optics	550 Meters	260 Meters	Not supported
1300nm Single-mode Optics	550 Meters	440 Meters	3000 Meters



For more information on 1000Base-SX and 1000Base-LX link characteristics, refer to IEEE Draft P802.3z/D3.1, Table 38-8.

LEDs

Table 1-2 describes the light emitting diode (LED) behavior on the Summit1.

Table 1-2: Summit1 LEDs

LED	Color	Indicates
Power	Green	The Summit1 is powered up.
	Yellow	The Summit1 is indicating a power, overheat, or fan failure.
MGMT	Green flashing	
	■ Slow	■ Power On Self Test (POST) in progress.
	■ Medium	■ The Summit1 is operating normally.
	■ Fast	■ Software download in progress.
	Yellow	The Summit1 has failed its POST.
Port Status LEDs		
Packet	Yellow	Frames are being transmitted/received on this port.
	Off	No activity on this port.
Status	Green on	Link is present; port is enabled; full-duplex operation.
	Green flashing	Link is present; port is disabled.
	Off	Link is not present.

SUMMIT2 FRONT VIEW

Figure 1-7 shows the Summit2 front view.

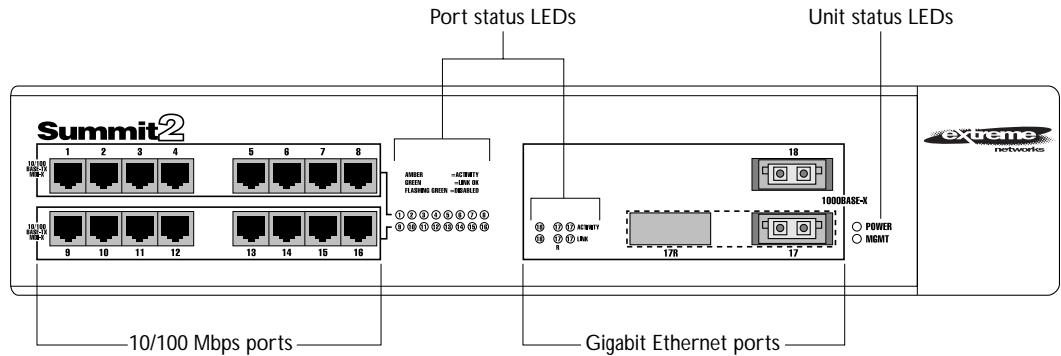


Figure 1-7: Summit2 front view

PORTS

The Summit2 has 16 autosensing 10Base-T/100Base-TX ports, two Gigabit Ethernet ports, one of which has a redundant Gigabit Ethernet port. Table 1-3 describes the ports, connectors, media, and maximum distances for each port type.

Table 1-3: Summit2 Supported Media

Media Module (Ports)	Connector	Media	Maximum Distance
RJ-45	RJ-45	Category 5 Cable (at 100Mbps) Category 3 Cable (at 10Mbps)	100 Meters
850nm Multimode Optics	SC	50u/125 Multimode Fiber 62.5u/125 Multimode Fiber	550 Meters 260 Meters
1300nm Singlemode Optics	SC	50u/125 Multimode Fiber 62.5u/125 Multimode Fiber 10u Singlemode Fiber	550 Meters 440 Meters 3000 Meters

LEDs

Table 1-4 describes the LED behavior on the Summit2.

Table 1-4: Summit2 LEDs

LED	Color	Indicates
Power	Green	The Summit2 is powered up.
	Yellow	The Summit2 is indicating a power, overheat, or fan failure.
MGMT	Green flashing	
	■ Slow	■ Power On Self Test (POST) in progress.
	■ Medium	■ The Summit2 is operating normally.
	■ Fast	■ Software download in progress.
	Yellow	The Summit2 has failed its POST.
10/100Mbps Port Status LEDs		
	Green	Link is present; port is enabled.
	Yellow	Frames are being transmitted/received on this port.
	Green flashing	Link is present; port is disabled.
	Off	Link is not present.
Gigabit Ethernet Port Status LEDs		
Packet	Yellow	Frames are being transmitted/received on this port.
	Off	No activity on this port.
Status	Green on	Link is present; port is enabled; full-duplex operation.
	Green flashing	Link is present; port is disabled.
	Off	Link is not present.

SUMMIT REAR VIEW

Figure 1-8 shows the rear view for the Summit1 and the Summit2.

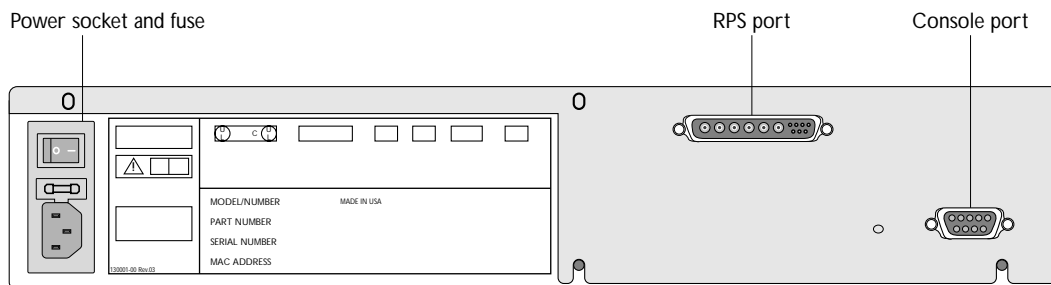


Figure 1-8: Summit rear view

POWER SOCKET

The Summit automatically adjusts to the supply voltage. The power supply operates down to 90 V. The fuse is suitable for both 110 V AC and 220-240 V AC operation.

SERIAL NUMBER

You may need this serial number for fault-reporting purposes.

CONSOLE PORT

Use the console port (9-pin, “D” type connector) for connecting a terminal and carrying out local out-of-band management.

REDUNDANT POWER SUPPLY PORT

The redundant power supply (RPS) port is used to connect to a Summit RPS. The Summit RPS provides a redundant power source to the Summit. If the primary power source for the Switch fails, the Summit RPS takes over, ensuring uninterrupted network operation.

In addition, when connected to a Summit RPS, the Summit Switch can provide status on power and fan operation of the RPS through SNMP and the command-line interface.

The Summit RPS can simultaneously provide power for up to two Summit Switches.

MAC ADDRESS

This label shows the unique Ethernet MAC address assigned to this device.

FACTORY DEFAULTS

Table 1-5 shows factory defaults for the Summit features.

Table 1-5: Summit Factory Defaults

Item	Default Setting
Port status	Enabled on all ports.
Serial or Telnet user account	<i>admin</i> with no password and <i>user</i> with no password.
Console port configuration	9600 baud, eight data bits, one stop bit, no parity, XON/XOFF flow control enabled.
Web network management	Enabled.
SNMP read community string	public.
SNMP write community string	private.
RMON history session	Enabled.
RMON alarms	Disabled.
BOOTP	Enabled on the default VLAN (<i>default</i>).
QoS	All traffic is part of the default queue.
802.1p priority	Recognition enabled.
Virtual LANs	One VLAN named <i>default</i> ; all ports belong to the default VLAN. The default VLAN belongs to the STPD named <i>s0</i> .
802.1Q tagging	All packets are untagged on the default VLAN (<i>default</i>)
Spanning Tree Protocol	Disabled; one STPD (<i>s0</i>).
IP Routing	Disabled.
Forwarding database aging period	300 seconds (5 minutes).

2

Installation and Setup

This chapter describes the following:

- How to decide where to install the Summit
- Gigabit Ethernet configuration rules
- How to install the Switch in a rack or free-standing
- How to connect equipment to the console port
- How to check the installation using the Power On Self-Test (POST)

FOLLOWING SAFETY INFORMATION

Before installing or removing any components of the Switch, or before carrying out any maintenance procedures, you must read the safety information provided in [Appendix A](#) of this guide.

DETERMINING THE SWITCH LOCATION

The Summit is suited for use in the office, where it can be free-standing or mounted in a standard 19-inch equipment rack. Alternatively, the device can be rack-mounted in a wiring closet or equipment room. Two mounting brackets are supplied with the Switch.

When deciding where to install the Switch, ensure that:

- The Switch is accessible and cables can be connected easily.
- Water or moisture cannot enter the case of the unit.
- Air-flow around the unit and through the vents in the side of the case is not restricted. You should provide a minimum of 25mm (1-inch) clearance.
- No objects are placed on top of the unit.
- Units are not stacked more than four high if the Switch is free-standing.

CONFIGURATION RULES

The connectors, supported media types, and maximum distances for the Summit family are described in [Chapter 1](#).

INSTALLING THE SUMMIT

The Summit can be mounted in a rack, or placed free-standing on a tabletop.

RACK MOUNTING

The Switch is 2U high and will fit in most standard 19-inch racks.



The rack mount kits must not be used to suspend the Switch from under a table or desk, or attach it to a wall.

To rack mount the Summit, follow these steps:

- 1 Place the Switch the right way up on a hard flat surface, with the front facing toward you.
- 2 Remove the existing screws from the sides of the chassis and retain for Step 4.
- 3 Locate a mounting bracket over the mounting holes on one side of the unit.
- 4 Insert the four screws and fully tighten with a suitable screwdriver, as shown in [Figure 2-1](#).

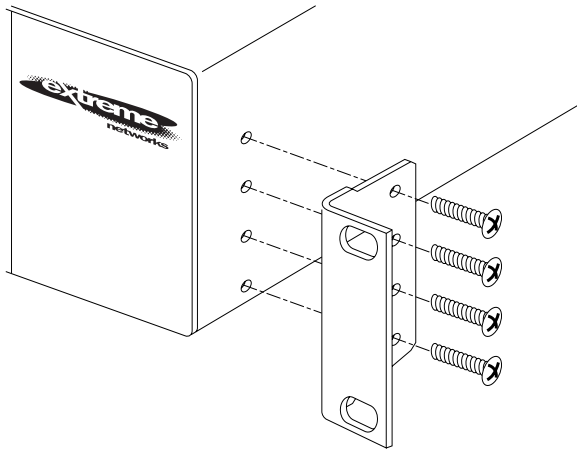


Figure 2-1: Fitting the mounting bracket

- 5 Repeat the three previous steps for the other side of the Switch.
- 6 Insert the Switch into the 19-inch rack and secure with suitable screws (not provided). Ensure that ventilation holes are not obstructed.
- 7 Connect the Summit to the redundant power supply (if applicable).
- 8 Connect cables.

FREE-STANDING

The Summit is supplied with four self-adhesive rubber pads. Apply the pads to the underside of the device by sticking a pad in the marked area at each corner of the Switch.

STACKING THE SWITCH AND OTHER DEVICES

Up to four units can be placed on top of one another.



This section relates only to physically placing the devices on top of one another. The Switch does not form a stack (that is, a number of devices linked together with special expansion cables to form a single logical device).

Apply the pads to the underside of the device by sticking a pad in the marked area at each corner of the Switch. Place the devices on top of one another, ensuring that the pads of the upper device line up with the recesses of the lower device.

CONNECTING EQUIPMENT TO THE CONSOLE PORT

Connection to the console port is used for direct local management. The Switch console port settings are set as follows:

- **Baud rate** — 9600
- **Data bits** — 8
- **Stop bit** — 1
- **Parity** — None
- **Flow control** — XON/XOFF

The terminal connected to the console port on the Switch must be configured with the same settings. This procedure will be described in the documentation supplied with the terminal.

Appropriate cables are available from your local supplier. In order to make your own cables, pin-outs for a DB-9 male console connector are described in [Table 2-1](#).

Table 2-1: Console Connector Pin-Outs

Function	Pin Number
TXD (transmit data)	3
RXD (receive data)	2
GND (ground)	5

[Figure 2-2](#) shows the pin-outs for a 9-pin to RS-232 25-pin null-modem cable.

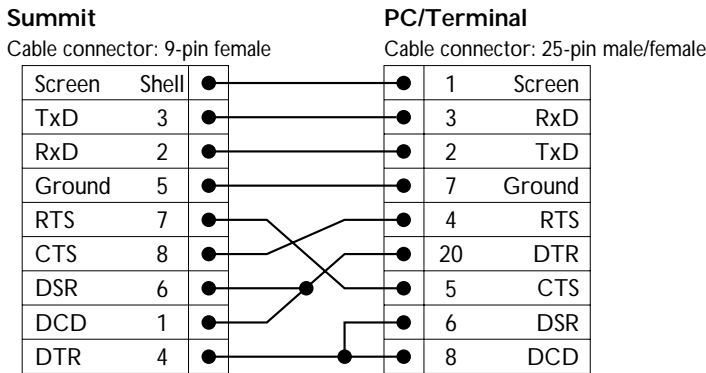


Figure 2-2: Null-modem cable pin-outs

Figure 2-3 shows the pin-outs for a 9-pin to 9-pin PC-AT null-modem serial cable.

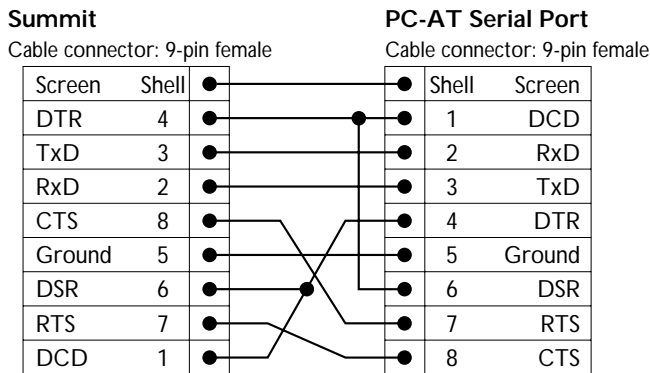


Figure 2-3: PC-AT serial null-modem cable pin-outs

POWERING-UP THE SWITCH

To turn on power to the Switch, connect the power cable to the Switch and then to the wall outlet, and turn the on/off switch to the on position.

CHECKING THE INSTALLATION

After turning on power to the Summit, the device performs a Power On Self-Test (POST).

During the POST, all ports are temporarily disabled, the packet LED is off, the power LED is on, and the MGMT LED flashes. The MGMT LED flashes until the Switch has successfully passed the POST.

If the Switch passes the POST, the MGMT LED blinks at a slow rate (1 blink per second). If the Switch fails the POST, the MGMT LED shows a solid yellow light.



For more information on the LEDs, refer to [Table 1-2](#) and [Table 1-4](#).

LOGGING IN FOR THE FIRST TIME

After the Summit has completed the POST, it is operational. Once operational, you can log in to the Switch and configure an IP address for the default VLAN (named *default*).

To manually configure the IP settings, perform the following steps:

- 1 Connect a terminal or workstation running terminal-emulation software to the console port.
- 2 At your terminal, press [Return] one or more times until you see the login prompt.
- 3 At the login prompt, enter the default user name *admin* to log on with administrator privileges. For example:

```
login: admin
```

Administrator capabilities allow you to access all Switch functions.



For more information on Switch security, refer to [Chapter 3](#).

- 4 At the password prompt, press [Return].
The default name, *admin*, has no password assigned. When you have successfully logged on to the Switch, the command-line prompt displays the name of the Switch in its prompt.
- 5 Assign an IP address and subnetwork mask for VLAN *default* by typing
config vlan default ipaddress 123.45.67.8 255.255.255.0
Your changes take effect immediately.
- 6 Save your configuration changes so that they will be in effect after the next Switch reboot, by typing

```
save
```



For more information on saving configuration changes, refer to [Chapter 11](#).

- 7 When you are finished using the facility, logout of the Switch by typing
logout



After two incorrect login attempts, the Summit locks you out of the login facility. You must wait a few minutes before attempting to log in again.

3

Accessing The Switch

This chapter provides the following required information to begin managing the Summit:

- Configuring the Switch for management
- Switch management methods
- Configuring SNMP
- Configuring Switch ports



*In order for configuration changes to be retained through a Switch power cycle or reboot, you must issue a **SAVE** command after you have made the change. For more information on the **SAVE** command, refer to [Chapter 11](#).*

CONFIGURING MANAGEMENT ACCESS

The Summit supports the following two level levels of management:

- User
- Administrator

A user-level account has viewing access to all manageable parameters, with the exception of the following:

- User account database
- SNMP community strings

A user-level account can use the `ping` command to test device reachability, and change the password assigned to the account name. If you have logged on with user capabilities, the command-line prompt will end with a (`>`) sign. For example:

```
Summit1:2>
```

An administrator-level account can view and change all Switch parameters. It can also add and delete users, and change the password associated with any account name. The administrator can disconnect a management session that has been established by way of a Telnet connection. If this happens, the user logged on by way of the Telnet connection is notified that the session has been terminated.

If you have logged on with administrator capabilities, the command-line prompt will end with a (`#`) sign. For example:

```
Summit1:18#
```

The prompt text is taken from the SNMP `sysname` setting. The number that follows the colon indicates the sequential line/command number.

If an asterisk (*) appears in front of the command-line prompt, it indicates that you have outstanding configuration changes that have not been saved. For example:

```
*Summit1:19#
```



For more information on saving configuration changes, refer to [Chapter 11](#).

DEFAULT ACCOUNTS

By default, the Switch is configured with two accounts, as shown in [Table 3-1](#).

Table 3-1: Default Accounts

Account Name	Access Level
admin	This user can access and change all manageable parameters. The admin account cannot be deleted.
user	<p>This user can view (but not change) all manageable parameters, with the following exceptions:</p> <ul style="list-style-type: none"> ■ This user cannot view the user account database. ■ This user cannot view the SNMP community strings. <p>This user has access to the <code>ping</code> command.</p>

CHANGING THE DEFAULT PASSWORD

Default accounts do not have passwords assigned to them. Passwords must have a minimum of 4 characters and can have a maximum of 12 characters.



Passwords are case-sensitive.

To add a password to the default admin account, follow these steps:

- 1 Log in to the Switch using the name *admin*.
- 2 At the password prompt, press [Return].
- 3 Add a default admin password by typing the following:
`config account admin`
- 4 Enter the new password at the prompt.
- 5 Re-enter the new password at the prompt.

To add a password to the default user account, follow these steps:

- 1 Log in to the Switch using the name *admin*.
- 2 At the password prompt, press [Return].
- 3 Add a default user password by typing the following:
`config account user`
- 4 Enter the new password at the prompt.
- 5 Re-enter the new password at the prompt.



If you forget your password while logged out of the command-line interface, contact your local technical support representative, who will advise on your next course of action.

CREATING A MANAGEMENT ACCOUNT

The Switch can have a total of three management accounts. You can use the default names (*admin* and *user*), or you can create new names and passwords for the accounts. Passwords must have a minimum of 4 characters and can have a maximum of 12 characters.



The account name “admin” cannot be deleted.

To create a new account, follow these steps:

- 1 Log in to the Switch as *admin*.
- 2 At the password prompt, press [Return].
- 3 Add a new user by using the following command:

```
create account [admin | user] <username>
```
- 4 Enter the password at the prompt.
- 5 Re-enter the password at the prompt.

VIEWING SWITCH ACCOUNTS

To view the accounts that have been created, you must have administrator privileges. Enter the following to see the accounts:

```
show account
```

Output from the show accounts command is as follows:

```
#show accounts
```

User Name	Access	LoginOK	Failed	Session
admin	R/W	0	0	
user	RO	0	0	

DELETING A SWITCH ACCOUNT

To delete a Switch account, you must have administrator privileges. Use the following command to delete an account:

```
delete account <username>
```

METHODS OF MANAGING THE SUMMIT

You can manage the Summit using the following methods:

- Access the command-line interface by connecting a terminal (or workstation with terminal-emulation software) to the Summit console port.
- Access the command-line interface over a TCP/IP network using a Telnet connection.

- Access the Web interface over a TCP/IP network, using a standard Web browser (such as Netscape Navigator™ 3.0 or greater, or Microsoft Internet Explorer™ 3.0 or greater).
- Use an SNMP Network Manager over a network running the IP protocol.

The Switch can support up to four user sessions concurrently (for example, one console port, one Web session, and two Telnet connections).

USING THE CONSOLE INTERFACE

The command-line interface built into the Switch is accessible by way of the 9-pin, RS-232 console port located on the rear of the unit.



For more information on the console port pin-outs, refer to [Chapter 2](#).

Once the connection is established, you will see the system prompt and you may log in.

USING TELNET

Any workstation with a Telnet facility should be able to communicate with the Switch over a TCP/IP network. Up to three active Telnet sessions can access the Switch concurrently. The Telnet connection will time out after three minutes of inactivity. If a connection to a Telnet session is lost inadvertently, the Switch terminates the session within three minutes.

Before you can start a Telnet session, you must set up the IP parameters described in the section “[Configuring Switch IP Parameters](#),” later in this chapter. Telnet is enabled by default.

To open the Telnet session, you must specify the IP address of the device that you want to manage. Check the user manual supplied with the Telnet facility if you are unsure of how to do this.

Once the connection is established, you will see the system prompt and you may log in.

CONFIGURING SWITCH IP PARAMETERS

In order to manage the Switch by way of a Telnet connection or by using an SNMP Network Manager, you must configure the Switch IP parameters.

USING A BOOTP SERVER

If you are using IP and you have a BOOTP server set up correctly on your network, you must add the following information to the BOOTP server:

- Switch Media Access Control (MAC) address
- IP address
- Subnet address mask (optional)
- Default gateway

The Switch MAC address is found on the rear label of the Switch.

Once this is done, the IP address, subnetwork mask, and default gateway for the Switch will be downloaded automatically. You can then start managing the Switch without further configuration.

You can enable BOOTP on a per-VLAN basis by using the following command:

```
enable bootp vlan [<name> | all]
```

By default, BOOTP is enabled on the default VLAN.

MANUALLY CONFIGURING THE IP SETTINGS

If you are using IP without a BOOTP server, you must enter the IP parameters for the Switch in order for the SNMP Network Manager or Telnet software to communicate with the device. To assign IP parameters to the Switch, you must do the following:

- Log in to the Switch with administrator privileges.
- Assign an IP address and subnetwork mask to a VLAN.

The Switch comes configured with a default VLAN named *default*. To use Telnet or an SNMP Network Manager, you must have at least one VLAN on the Switch, and it must be assigned an IP address and subnetwork mask. IP addresses are always assigned to a VLAN. The Summit can be assigned multiple IP addresses.



For information on creating and configuring VLANs, refer to [Chapter 5](#).

To manually configure the IP settings, perform the following steps:

- 1 Connect a terminal or workstation running terminal emulation software to the console port.
- 2 At your terminal, press [Return] one or more times until you see the login prompt.

- 3 At the login prompt, enter your user name and password. Note that they are both case-sensitive. Ensure that you have entered a user name and password with administrator privileges.

- If you are logging in for the first time, use the default user name *admin* to log in with administrator privileges. For example:

```
login: admin
```

Administrator capabilities enable you to access all Switch functions. The default user names have no passwords assigned. For more information on switch security, refer to “[Configuring Management Access](#),” on [page 3-1](#).

- If you have been assigned a user name and password with administrator privileges, enter them at the login prompt.

- 4 At the password prompt, enter the password and press [Return].

When you have successfully logged in to the Switch, the command-line prompt displays the name of the Switch in its prompt.

- 5 Assign an IP address and subnetwork mask for the default VLAN by using the following command:

```
config vlan <name> ipaddress <ipaddress> {<subnet_mask>} {<metric>}
```

For example:

```
config vlan default ipaddress 123.45.67.8 255.255.255.0 1
```

Your changes take effect immediately.

- 6 Configure the default route for the Switch using the following command:

```
config iproute add default <ipaddress> {<metric>}
```

For example:

```
config iproute add default 123.0.0.1
```

- 7 Save your configuration changes so that they will be in effect after the next Switch reboot, by typing

```
save
```



For more information on saving configuration changes, refer to [Chapter 11](#).

- 8 When you are finished using the facility, log out of the Switch by typing

```
logout
```

DISCONNECTING A TELNET SESSION

The administrator-level account can disconnect a management session that has been established by way of a Telnet connection. If this happens, the user logged in by way of the Telnet connection is notified that the session has been terminated.

To terminate a Telnet session, follow these steps:

- 1 Log in to the Switch with administrator privileges.
- 2 Determine the session number of the session you want to terminate by typing

```
show session
```

Sample output from the `show session` command is as follows:

```
show session:
```

```
0  Wed Sep 17 20:48:38 1997  admin  console serial
4  Wed Sep 17 21:52:16 1997  admin  telnet 192.208.37.26
```

- 3 Terminate the session by using the following command:

```
clear session <session_number>
```

DISABLING TELNET ACCESS

By default, Telnet services are enabled on the Switch. You can choose to disable Telnet by entering

```
disable telnet
```

To re-enable Telnet on the Switch, at the console port enter

```
enable telnet
```

You must be logged in as an administrator to enable or disable Telnet.

USING THE WEB INTERFACE

Any properly configured standard Web browser that supports frames (such as Netscape Navigator 3.0 or Microsoft Internet Explorer 3.0) can manage the Switch over a TCP/IP network. To use the Web interface, at least one VLAN on the Switch must be assigned an IP address.



For more information on assigning an IP address, refer to [“Configuring Switch IP Parameters,”](#) on [page 3-5](#).

The default home page of the Switch can be accessed using the following address:

`http://<ipaddress>`

When you access the home page of the Switch, you are presented with the Logon screen.

SUMMIT MANAGEMENT INTERFACE SCREEN

After logging in to the Switch, the Web interface presents the Summit Management Interface Screen. From this page, you have the following options:

- Configuration
- Statistics
- Support
- Logout

CONFIGURATION

The Configuration option enables you to view and configure settings for Switch functions, including the following:

- Switch functions
- User accounts
- VLANs
- Ports
- QoS
- STP
- Error Log

STATISTICS

The Statistics option provides access to Switch statistics, including the following:

- Port statistics
- Port errors

- ICMP statistics
- RIP statistics

SUPPORT

The Support option includes the following features:

- Upgrade software
- Contact Support

LOGOUT

The Logout option ends your management session, and returns you to the Logon page.

DISABLING WEB ACCESS

By default, web access is enabled on the Summit. To disable it, enter the following command:

```
disable web
```

To re-enable web access, enter the following command:

```
enable web
```

You will need to reboot the Switch in order for these changes to take effect. For more information on rebooting the Switch, refer to [Chapter 11](#).

USING SNMP

Any Network Manager running the Simple Network Management Protocol (SNMP) can manage the Switch, provided the Management Information Base (MIB) is installed correctly on the management station. Each Network Manager provides its own user interface to the management facilities.

The following sections describe how to get started if you want to use an SNMP manager. It assumes you are already familiar with SNMP management. If not, refer to the following publication:

“The Simple Book”
by Marshall T. Rose
ISBN 0-13-8121611-9
Published by Prentice Hall

ACCESSING SWITCH AGENTS

In order to have access to the SNMP agent residing in the Switch, at least one VLAN must have an IP address assigned to it.

SUPPORTED MIBs

Any Network Manager running SNMP can manage the Summit, provided the MIB is installed correctly on the management station. In addition to private MIBs, the Summit supports the standard MIBs listed in [Table 3-2](#).

Table 3-2: Supported MIBs

Description	RFC Number
MIB II	1213
Bridge MIB	1493
RMON (Etherstats, History, Alarms, and Events)	1757
RMON II Probe Configuration	2021
Evolution of Interfaces	1573

CONFIGURING SNMP SETTINGS

The following SNMP parameters can be configured on the Switch:

- **Authorized trap receivers** — An authorized trap receiver can be one or more network management stations on your network. The Switch sends SNMP traps to the trap receiver. You can have a maximum of six trap receivers configured for each Summit.

- **Authorized managers** — An authorized manager can be one or more network management stations on your network. The Summit can have a maximum of six authorized managers.
- **Community strings** — The community strings allow a simple method of authentication between the Switch and the remote Network Manager. There are two community strings on the Summit. The *read community string* provides read-only access to the switch. The default read community string is *public*. The *write community string* provides read and write access to the Switch. The default write community string is *private*. The community string for all authorized trap receivers must be configured on the Switch for the trap receiver to receive Switch-generated traps.
- **System contact** (optional) — The system contact is a text field that enables you to enter the name of the person(s) responsible for managing the Switch.
- **System name** — The system name is the name that you have assigned to this Switch. The default name is Summit1 or Summit2.
- **System location** (optional) — Using the system location field, you can enter an optional location for this Switch.

Table 3-3 describes SNMP configuration commands.

Table 3-3: SNMP Configuration Commands

Command	Description
config vlan <name> ipaddress <ip_address> {<mask>}	Configures an IP address for the VLAN. This is required in order to use an SNMP manager.
config iproute add default <ip_address> {<mask>} {<metric>}	Configures the default gateway for the switch. A default gateway must be on a configured IP interface.
enable snmp access	Turns on SNMP support for the Switch.
enable snmp trap	Turns on SNMP trap support.
config snmp add <ipaddress>	Adds the IP address of an SNMP management station to the access list. Up to six addresses can be specified.
config snmp add trapreceiver <ipaddress> {community <string>}	Adds the IP address of a specified trap receiver. A maximum of six trap receivers is allowed.
config snmp community [read readwrite] <string>	Configures the SNMP read and write community strings. The community string can have a maximum of 127 characters.

Table 3-3: SNMP Configuration Commands (continued)

Command	Description
<code>config snmp delete [<ipaddress> all]</code>	Deletes the IP address of a specified SNMP management station or all SNMP management stations.
<code>config snmp delete trapreceiver [<ip_address> community <string> all]</code>	Deletes the IP address of a specified trap receiver or all authorized trap receivers. If you delete all trap receiver addresses, any machine can have SNMP management access to the Switch.
<code>config snmp syscontact <string></code>	Configures the name of the system contact. A maximum of 255 characters is allowed.
<code>config snmp sysname <string></code>	Configures the name of the Switch. A maximum of 255 characters is allowed. The default sysname is <i>Summit</i> . The system name in the Summit prompt.
<code>config snmp syslocation <string></code>	Configures the location of the Switch. A maximum of 255 characters is allowed.

DISPLAYING SNMP SETTINGS

To display the SNMP settings configured on the Summit, enter the following command:

show management

This command displays the following information:

- Enable/disable state for telnet, SNMP, and Web access
- SNMP community strings
- Authorized SNMP station list
- SNMP trap receiver list
- Login statistics

RESETTING AND DISABLING SNMP

To reset and disable SNMP settings, use the commands in [Table 3-4](#).

Table 3-4: SNMP Reset and Disable Commands

Command	Description
disable snmp access	Disables SNMP on the Switch.
disable snmp trap	Prevents SNMP traps from being sent from the Switch. Does not clear the SNMP trap receivers that have been configured.
unconfig management	Restores default values to all SNMP-related entries.

CHECKING BASIC CONNECTIVITY

The Summit offers the following two commands for checking basic connectivity:

- ping
- traceroute

PING

The `ping` command enables you to send Internet Control Message Protocol (ICMP) echo messages to a remote IP device. The `ping` command is available for both the user and administrator privilege level.

The `ping` command syntax is as follows.

```
ping {continuous} {size <n>} <ip_address>
```

Options for the `ping` command are described in [Table 3-5](#).

Table 3-5: Ping Command Parameters

Parameter	Description
continuous	Specifies ICMP echo messages to be sent continuously. This option can be interrupted by pressing any key.
size <n>	Specifies the size of the packet.

TRACEROUTE

The `traceroute` command enables you to trace the routed path between the Switch and a destination endstation. The `traceroute` command syntax is as follows:

```
traceroute <ip_address>
```

where the `ip_address` is the IP address of the destination endstation.

CONFIGURING PORTS

Ports on the Summit1 and Summit2 can be configured in the following ways:

- Enabling and disabling individual ports
- Configuring the port speed (Summit2 only)
- Configuring half- or full-duplex mode
- Creating load-sharing groups on multiple ports
- Changing the Quality or Service (QoS) setting for individual ports



For more information on QoS, refer to [Chapter 8](#).

ENABLING AND DISABLING PORTS

By default, all ports are enabled. To enable or disable one or more ports, use the following command:

```
[enable | disable] port <portlist>
```

For example, to disable ports 3, 5, and 12 through 15 on the Summit2, enter the following:

```
disable port 3,5,12-15
```

Even though a port is disabled, the link remains enabled for diagnostic purposes.

CONFIGURING PORT SPEED AND DUPLEX SETTING

By default, the Summit is configured to use autonegotiation to determine the port speed and duplex setting for each port. You can select to manually configure the duplex setting and the speed of the 10/100 Mbps ports on the Summit2, and you can manually configure the duplex setting on the Summit1.

Ports 1 through 16 on the Summit2 can connect to either 10Base-T or 100Base-T networks. By default, the ports autonegotiate port speed. You can also configure each port for a particular speed (either 10 Mbps or 100 Mbps).

Gigabit Ethernet ports on both the Summit1 and the Summit2 are statically set to 1 Gbps, and their speed cannot be modified.

All ports on the Summit1 and Summit2 can be configured for half-duplex or full-duplex operation. By default, the ports autonegotiate the duplex setting.

To configure port speed and duplex setting, use the following command:

```
config port <portlist> auto off {speed [10 | 100]} duplex [half | full]
```

To configure the Switch to autonegotiate, use the following command:

```
config port <portlist> auto on
```

PORT COMMANDS

[Table 3-6](#) describes the port commands.

Table 3-6: Port Commands

Command	Description
config port <portlist> auto on	Enables autonegotiation for the particular port type; 802.3u for 10/100 Mbps ports or 802.3z for Gigabit Ethernet ports.


Table 3-6: Port Commands (continued)

Command	Description
config port <portlist> auto off {speed [10 100]} duplex [half full]	<p>Changes the configuration of a group of ports. Specify the following:</p> <ul style="list-style-type: none"> ■ <code>auto off</code> — the port will not autonegotiate the settings ■ <code>speed</code> — the speed of the port (for 10/100 Mbps ports on the Summit2, only) ■ <code>duplex</code> — the duplex setting (half- or full-duplex)
config port <portlist> qosprofile <qosname>	<p>Configures one or more ports to use a particular QoS profile.</p> <p>For more information on QoS, refer to Chapter 8.</p>
enable port <portlist>	Enables a port.
disable port <portlist>	Disables a port. Even when disabled, the link is available for diagnostic purposes.
enable smartredundancy <portlist>	Enables the smart redundancy feature on the Summit2 redundant Gigabit Ethernet port. When the smart redundancy feature is enabled, the Switch always uses the primary link when the primary link is available.
disable smartredundancy <portlist>	Disables the smart redundancy feature on the Summit2. If the feature is disabled, the Switch changes the active link only when the current active link becomes inoperable.
show port <portlist> config	Displays the port configuration.
show port <portlist> stats	Displays real-time port statistics. For more information on port statistics, refer to Chapter 10 .
show port <portlist> errors	Displays real-time error statistics. For more information on error statistics, refer to Chapter 10 .
show port <portlist> collisions	Displays real-time collision statistics.
show port <portlist> packet	Displays a histogram of packet statistics.

4 Commands

This chapter contains a description of each command-line interface command for the Summit. It also provides the following information related to Summit commands:

- Command syntax
- Line-editing commands
- Command history substitution

 *In order for configuration changes to be retained through a Switch power cycle or reboot, you must issue a SAVE command after you have made the change. For more information on the SAVE command, refer to [Chapter 11](#).*

UNDERSTANDING THE COMMAND SYNTAX

This section describes the steps to take when entering a command. Refer to the sections that follow for detailed information on using the command-line interface.

To use the command-line interface, follow these steps:

- 1 When entering a command at the prompt, ensure that you have the appropriate privilege level.
Most configuration commands require you to have the administrator privilege level.
- 2 Enter the command name.
If the command does not include a parameter or values, skip to Step 3. If the command requires more information, or if you want to include optional arguments, continue to Step 2a.

- a If the command has additional options, include them after the command name.
 - b If the command includes a parameter, enter the parameter name and values.
The value part of the command specifies how you want the parameter to be set.
Values include numerics, strings, or addresses, depending on the parameter.
- 3 After entering the complete command, press [Return].



If an asterisk () appears in front of the command-line prompt, it indicates that you have outstanding configuration changes that have not been saved. For more information on saving configuration changes, refer to [Chapter 11](#).*

SYNTAX HELPER

The command-line interface has a built-in syntax helper. If you are unsure of the complete syntax for a particular command, enter as much of the command as possible. The syntax helper provides a list of options for the remainder of the command.

The syntax helper also provides assistance if you have entered an incorrect command.

COMMAND COMPLETION

The Summit provides command completion by way of the [Tab] key. If you enter the beginning of a unique command, pressing [Tab] forces the Summit to fill in the remainder of the command.

ABBREVIATED SYNTAX

Abbreviated syntax is the shortest, most unambiguous, allowable abbreviation of a command, parameter, or value. Typically, this is the first three letters of the command.

COMMAND SHORTCUTS

All named components of the Switch configuration must have a unique name. Components are named using the `create` command. When you enter a command to configure a named component, you do not need to use the keyword of the component. For example, to create a VLAN, you must enter a unique VLAN name:

```
create vlan engineering
```

Once you have created the VLAN with a unique name, you can then eliminate the keyword `vlan` from all other commands that require the name to be entered. For example, instead of entering the command

```
config vlan engineering add port 1-3,6
```

you could enter the following shortcut:

```
config engineering add port 1-3, 6
```

NUMERICAL RANGES

Commands that require you to enter one or more port numbers use the parameter `<portlist>` in the syntax. A portlist can be a range of numbers, for example:

```
port 1-3
```

You can add additional port numbers to the list, separated by a comma:

```
port 1-3,6,8
```

NAMES

All named components of the Switch configuration must have a unique name. Names must begin with an alphabetical character delimited by whitespace, unless enclosed in quotation marks.

SYMBOLS

You may see a variety of symbols shown as part of the command syntax. These symbols explain how to enter the command, and you do not type them as part of the command itself. [Table 4-1](#) summarizes command syntax symbols.

Table 4-1: Command Syntax Symbols

Symbol	Description
angle brackets <code>< ></code>	Enclose a variable or value. You must specify the variable or value. For example, in the syntax <pre>config vlan <name> ipaddress <ip_address></pre> you must supply a VLAN name for <code><name></code> and an address for <code><ip_address></code> when entering the command. Do not type the angle brackets.

Table 4-1: Command Syntax Symbols (continued)

Symbol	Description
square brackets []	<p>Enclose a required value or list of required arguments. One or more values or arguments can be specified. For example, in the syntax</p> <pre>disable vlan [<name> all]</pre> <p>you must specify either the VLAN name for <name>, or the keyword <code>all</code> when entering the command. Do not type the square brackets.</p>
vertical bar	<p>Separates mutually exclusive items in a list, one of which must be entered. For example, in the syntax</p> <pre>config snmp community [read write] <string></pre> <p>you must specify either the <code>read</code> or <code>write</code> community string in the command. Do not type the vertical bar.</p>
braces { }	<p>Enclose an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax</p> <pre>show vlan {<name> all}</pre> <p>you can specify either a particular VLAN or the keyword <code>all</code>. If you do not specify an argument, the command will show all VLANs. Do not type the braces.</p>

LINE-EDITING KEYS

[Table 4-2](#) describes the line-editing keys available using the command-line interface.

Table 4-2: Line-Editing Keys

Key(s)	Description
Backspace	Deletes character to the left of cursor and shifts remainder of line to left.
Delete or [Ctrl]+D	Deletes character under cursor and shifts remainder of line to left.
[Ctrl] + K	Deletes characters from under cursor to the end of the line.
Insert	Toggles on and off. When toggled on, inserts text and pushes previous text to right.
Left Arrow	Moves cursor to left.
Right Arrow	Moves cursor to right.
Home or [Ctrl]+A	Moves cursor to first character in line.
End or [Ctrl]+E	Moves cursor to last character in line.
[Ctrl]+L	Clears the screen and moves the cursor to the beginning of the line.

Table 4-2: Line-Editing Keys (continued)

Key(s)	Description
Up Arrow	Displays the previous command in the command history buffer, and places cursor at end of command.
Down Arrow	Displays the next command in the command history buffer, and places cursor at end of command.

COMMAND HISTORY

The Summit “remembers” the last 50 commands you enter. You can display a list of these commands by using the following command:

```
history
```

COMMON COMMANDS

[Table 4-3](#) describes common commands used to manage the Switch. Commands specific to a particular feature are described in the other chapters of this guide.

Table 4-3: Common Commands

Command	Description
create account [admin user] <username> {<password>}	Creates a user account. For more information on creating accounts, refer to Chapter 3 .
create vlan <name>	Creates a VLAN. For more information on VLANs, refer to Chapter 5 .
config account <username> {<password>}	Configures a user account password.

Table 4-3: Common Commands (continued)

Command	Description
config devicemode [bridging iprouting ipmc]	<p>Configures the operating mode of the Switch. Specify:</p> <ul style="list-style-type: none"> ■ <code>bridging</code> — Layer 2 bridging functions only ■ <code>iprouting</code> — Bridging and IP unicast routing functions ■ <code>ipmc</code> — Bridging, IP unicast routing, and IP multicast routing functions <p>If this command is used to change the operating mode of the Summit once it is up and running, it causes the Switch to save the configuration and reboot. The default operating mode is <code>iprouting</code>.</p>
config port <portlist> auto off {speed [10 100]} duplex [half full]	Manually configures the port speed and duplex setting of one or more ports. For more information on configuring ports, refer to Chapter 3 .
config time <time>	<p>Configures the system date and time. The format for <time> is:</p> <pre>mm/dd/yyyy hh:mm:ss</pre> <p>The time uses a 24-hour clock format.</p>
config vlan <name> ipaddress <ip_address> {<mask>}	Configures an IP address and subnet mask for a VLAN.
enable bootp vlan [<name> all]	Enables BOOTP for one or more VLANs. For more information on using BOOTP, refer to Chapter 3 .
clear session <number>	Terminates a Telnet session from the Switch.
disable bootp vlan [<name> all]	Disables BOOTP for one or more VLANs.
disable port <portlist>	Disables a port.
disable telnet	Disables Telnet access to the Switch.
disable web	Disables web access to the Switch.
delete account <username>	Deletes a user account.
delete vlan <name>	Deletes a VLAN.

Table 4-3: Common Commands (continued)

Command	Description
unconfig switch {all}	Resets all switch parameters (with the exception of defined user accounts) to the factory defaults. If you specify the keyword <code>all</code> , the user account information is reset as well.

SUMMIT COMMANDS

The tables in this section list all of the commands used on the Summit Switch. The commands are organized by the following categories:

- General Switch commands
- User account commands
- Switch management commands
- VLAN commands
- Protocol commands
- FDB commands
- Port commands
- STP commands
- QoS commands
- Basic IP commands
- IP ARP commands
- IP Route Table commands
- ICMP commands
- RIP commands
- Logging commands
- Configuration and image commands

GENERAL SWITCH COMMANDS

Table 4-4 describes general Switch commands.

Table 4-4: General Switch Commands

Command	Description
show switch	<p>Displays the current Switch information, including:</p> <ul style="list-style-type: none">■ sysName, sysLocation, sysContact■ MAC address■ Current date and time, and system uptime■ Operating environment (temperature, fans, and power supply status)■ Nonvolatile Random Access Memory (NVRAM) image information (primary/secondary image, date, time, size, version)■ NVRAM configuration information (primary/secondary configuration, date, time, size, version)■ Scheduled reboot information■ System serial number and reworks indicator■ Software platform■ System ID■ Power supply and fan status
show version	<p>Displays the hardware and software versions currently running on the Switch. Also displays the Switch serial number.</p>
show memory	<p>Displays the current system memory information.</p>
reboot {<time>}	<p>Reboots the Switch at the time specified. If no time is specified, the Switch reboots immediately following the command.</p>
config time <time>	<p>Configures the system date and time. The format for <time> is:</p> <p>mm/dd/yyyy hh:mm:ss</p> <p>The time uses a 24-hour clock format.</p>

Table 4-4: General Switch Commands (continued)

Command	Description
config devicemode [bridging iprouting]	<p>Configures the operating mode of the Switch. Specify:</p> <ul style="list-style-type: none"> ■ <code>bridging</code> — Layer 2 bridging functions only ■ <code>iprouting</code> — Bridging and IP unicast routing functions <p>If this command is used to change the operating mode of the Summit once it is up and running, it causes the Switch to save the configuration and reboot. The default operating mode is <code>iprouting</code>.</p>
unconfig switch {all}	<p>Resets all Switch parameters (with the exception of defined VLANs and IP addresses) to the factory defaults. If you specify the keyword <code>all</code>, the IP addresses are reset as well.</p>
ping {continuous} {size <number>} <ipaddress>	<p>Sends ICMP echo messages to a remote IP device. Specify:</p> <ul style="list-style-type: none"> ■ <code>continuous</code> — ICMP echo messages should be sent continuously. ■ <code>size <n></code> — The size of the packet. <p>The <code>continuous</code> option can be interrupted by pressing any key.</p>
traceroute <ipaddress>	<p>Traces the routed path between the Switch and a destination endstation.</p>
clear counters	<p>Clears all statistical counters for the Switch and ports.</p>

USER ACCOUNT COMMANDS

[Table 4-5](#) describes user account commands.

Table 4-5: User Account Commands

Command	Description
show account	Displays the account names, access level, number of successful and failed login attempts, and the number of active sessions in the user database. This command is available only to admin level users.
create account [admin user] <username> {<password>}	Creates a user account.
delete account <username>	Deletes a user account
config account <username> {<password>}	Changes the password of an existing account.

SWITCH MANAGEMENT COMMANDS

Table 4-6 describes Switch management commands.

Table 4-6: Switch Management Commands

Command	Description
show management	Displays network management configuration and statistics, including enable/disable states for Telnet and SNMP, SNMP community strings, authorized SNMP station list, SNMP trap receiver list, and login statistics.
show session	Displays the currently active Telnet and console sessions communicating with the Switch. Provides the user name, IP address of the incoming Telnet session, whether a console session is currently active, and login time. Sessions are numbered.
clear session <number>	Terminates a Telnet session from the Switch.
logout quit	Logs out of a console or Telnet session. If used during a Telnet session, also closes the TCP Telnet session.
enable telnet	Enables Telnet access to the Switch.
disable telnet	Disables Telnet access to the Switch.
enable web	Enables web access to the Switch. Requires a reboot to take effect.

Table 4-6: Switch Management Commands (continued)

Command	Description
disable web	Disables web access to the Switch. Requires a reboot to take effect.
enable snmp access	Turns on SNMP support for the Switch.
disable snmp access	Disables SNMP on the Switch.
enable snmp trap	Turns on SNMP trap support.
disable snmp trap	Prevents SNMP traps from being sent from the Switch. Does not clear the SNMP trap receivers that have been configured.
config snmp add <ipaddress>	Adds the IP address of an SNMP management station to the access list. Up to six addresses can be specified.
config snmp delete [<ipaddress all]	Deletes the IP address of a specified SNMP management station or all SNMP management stations.
config snmp add trapreceiver <ipaddress> {<comm_string>}	Adds the IP address of a specified trap receiver. A maximum of six trap receivers is allowed.
config snmp delete trapreceiver [<ip_address> community <string> all]	Deletes the IP address of a specified trap receiver or all authorized trap receivers. If you delete all trap receiver addresses, any machine can have SNMP management access to the Switch.
config snmp community [read readwrite] <string>	Configures the SNMP read and write community strings. The community string can have a maximum of 127 characters.
config snmp syscontact <string>	Configures the name of the system contact. A maximum of 255 characters is allowed.
config snmp sysname <string>	Configures the name of the Switch. The <i>sysname</i> appears in the command-line interface prompt. A maximum of 255 characters is allowed. The default <i>sysname</i> is Summit1 or Summit2.
config snmp syslocation <string>	Configures the location of the Switch. A maximum of 255 characters is allowed.
unconfig management	Restores default values to all SNMP-related entries.

VLAN COMMANDS

Table 4-7 describes VLAN commands.

Table 4-7: VLAN Commands

Command	Description
show vlan {<name> all}	When used with the keyword <code>all</code> , or with no named VLANs, displays a summary list of VLAN names with a portlist and associated status of each. When used with a named identifier, displays port information, including membership list, IP address, and tag information.
create vlan <name>	Creates a named VLAN.
delete vlan <name>	Removes a VLAN.
config vlan <name> [add delete] port <portlist> {tagged untagged}	Adds and deletes ports. You can specify tagged and untagged port(s). By default, ports are untagged.
config vlan <name> tag <vlanid>	Assigns a numerical VLANid. The valid range is from 1 to 4095.
config vlan <name> protocol [<protocol_name> any]	Configures a protocol-based VLAN. If the keyword <code>any</code> is specified, then it becomes the default VLAN. All packets that cannot be classified into other protocol-based VLANs are assigned to the default VLAN of that port.
config vlan <name> qosprofile <qosname>	Configures a VLAN to use a particular QoS profile. Dynamic FDB entries associated with the VLAN are flushed once this change is committed.
config vlan <name> ipaddress <ipaddress> {<mask>}	Assigns an IP address and an optional mask to the VLAN.
config dot1q ethertype <ethertype>	Configures an IEEE 802.1Q Ethertype. Use this command if you have another Switch that supports 802.1Q, but uses a different Ethertype. The default value used by the Switch is 8100.
unconfig vlan <name> ipaddress	Removes the IP address associated with a VLAN.

PROTOCOL COMMANDS

Table 4-8 describes protocol commands.

Table 4-8: Protocol Commands

Command	Description
show protocol {<protocol_name> all}	Displays protocol-related information, including: <ul style="list-style-type: none"> ■ Protocol name ■ List of protocol fields ■ List of VLANs that use this protocol
create protocol <protocol _ name>	Creates a user-defined protocol.
delete protocol <protocol_name>	Removes a protocol.
config protocol <protocol_name> [add delete] <prototype_number> {<prototype_number>} ...	Configures a protocol filter. Supported protocol types include: <ul style="list-style-type: none"> ■ EtherType ■ LLC ■ SNAP

FDB COMMANDS

Table 4-9 describes FDB commands.

Table 4-9: FDB Commands

Command	Description
show fdb {all <mac_address> vlan <name> <portlist> permanent}	Displays the forwarding database contents including MAC address, associated VLAN, port, age-of-entry configuration method, and status. Providing one of the options acts as a filter on the display. Providing a VLAN name displays all entries for the VLAN. Use the MAC address to locate a specific entry in the FDB.
clear fdb {all <mac_address> vlan <name> <portlist> }	Clears dynamic FDB entries that match the filter. Use the keyword <code>all</code> to clear all dynamic entries.

Table 4-9: FDB Commands (continued)

Command	Description
create fdbentry <mac_address> vlan <name> <portlist>	<p>Creates a permanent FDB entry. Specify the following:</p> <ul style="list-style-type: none"> ■ <code>mac_address</code> — Device MAC address, using colon-separated bytes. ■ <code>name</code> — VLAN associated with MAC address. ■ <code>portlist</code> — Port number associated with MAC address. <p>If more than one port number is associated with a permanent MAC entry, packets are multicast to the multiple destinations.</p>
delete fdbentry <mac_address> vlan <name>	Deletes a permanent FDB entry.
config fdb agingtime <number>	Configures the FDB aging time. The range is 15 through 1,000,000 seconds. The default value is 1,800 seconds. A value of 0 indicates that the entry should never be aged out.

PORT COMMANDS

[Table 4-10](#) describes port commands.

Table 4-10: Port Commands

Command	Description
show port <portlist> config	Displays state, link status, speed, and autonegotiation setting for each port.
show port <portlist> stats	Displays port information including physical layer configuration and statistics.
show port <portlist> errors	Displays error information for one or more ports.
show port <portlist> collisions	Displays real-time collision statistics.
show port <portlist> packet	Displays a histogram of packet statistics for one or more ports.
config port <portlist> auto on	enables autonegotiation for the particular port type: 802.3u for 10/100 Mbps ports or 802.3z for Gigabit Ethernet ports.

Table 4-10: Port Commands

Command	Description
config port <portlist> auto off {speed [10 100]} duplex [half full]	Changes the configuration of a group of ports. Specify the following: <ul style="list-style-type: none"> ■ <code>auto off</code> — The port will not autonegotiate the settings. ■ <code>speed</code> — The speed of the port (for 10/100 Mbps ports on the Summit2, only). ■ <code>duplex</code> — The duplex setting (half- or full-duplex).
config port <portlist> qosprofile <qosname>	Configures one or more ports to use a particular QoS profile.
enable port <portlist>	Enables one or more ports.
disable port <portlist>	Disables one or more ports.
enable smartredundancy <portlist>	Enables smart redundancy on the Summit2 redundant Gigabit Ethernet port.
disable smartredundancy <portlist>	Disables smart redundancy on the Summit2.

STP COMMANDS

[Table 4-11](#) describes STP commands.

Table 4-11: STP Commands

Command	Description
show stpd {<stpd_name> all}	Displays STP information for one or all STPDs on the Switch.
show stpd <stpd_name> port <portlist>	Displays port-specific STP information.
create stpd <stpd_name>	Creates an STPD. When created, an STPD has the following default parameters: <ul style="list-style-type: none"> ■ Bridge priority — 32,768 ■ Hello time — 2 seconds ■ Forward delay — 15 seconds
delete stpd <stpd_name>	Removes an STPD. An STPD can only be removed if all VLANs have been deleted from it.
config stpd <stpd_name> add vlan <name>	Adds a VLAN to the STPD.

Table 4-11: STP Commands (continued)

Command	Description
config stpd <stpd_name> delete vlan [<name> all]	Removes one or all VLANs from an STPD. If all is specified, the association between the STPD and VLAN is removed, but both are still instantiated.
config stpd <stpd_name> hellotime <value>	Specifies the time delay (in seconds) between the transmission of BPDUs from this STPD when it is the Root Bridge. The range is 1 through 10. The default setting is 2 seconds.
config stpd <stpd_name> forwarddelay <value>	Specifies the time (in seconds) that the ports in this STPD spend in the listening and learning states when the Switch is the Root Bridge. The range is 4 through 30. The default setting is 15 seconds.
config stpd <stpd_name> maxage <value>	Specifies the maximum age of a BPDU in this STPD. The range is 6 through 40. The default setting is 20 seconds. Note that the time must be greater than, or equal to $2 \times (\text{Hello Time} + 1)$ and less than, or equal to $2 \times (\text{Forward Delay} - 1)$.
config stpd <stpd_name> priority <value>	Specifies the priority of the STPD. By changing the priority of the STPD, you can make it more or less likely to become the Root Bridge. The range is 0 through 65,535. The default setting is 32,768. A setting of 0 indicates the highest priority.
config stpd <stpd_name> port cost <value> <portlist>	Specifies the path cost of the port in this STPD. The range is 1 through 65,535. The Switch automatically assigns a default path cost based on the speed of the port, as follows: <ul style="list-style-type: none"> ■ For a 10Mbps port, the default cost is 100. ■ For a 100Mbps port, the default cost is 19. ■ For a 1000Mbps port, the default cost is 4.

Table 4-11: STP Commands (continued)

Command	Description
config stpd <stpd_name> port priority <value> <portlist>	Specifies the priority of the port in this STPD. By changing the priority of the port, you can make it more or less likely to become the Root Port. The range is 0 through 255. The default setting is 128. A setting of 0 indicates the lowest priority.
enable stpd [<stpd_name> all]	Enables the STP protocol for one or all STPDs. The default setting is disabled.
disable stpd [<stpd_name> all]	Disables the STP mechanism on a particular STPD, or for all STPDs.
enable stpd port <portlist>	Enables the STP protocol on one or more ports. If STPD is enabled for a port, BPDUs will be generated on that port if STP is enabled for the associated STPD. The default setting is enabled.
disable stpd port <portlist>	Disables STP on one or more ports. Disabling STP on one or more ports puts those ports in FORWARDING state; all BPDUs received on those ports will be disregarded.
unconfig stpd {<stpd_name> all}	Restores default STP values to a particular STPD or to all STPDs.

QoS COMMANDS

[Table 4-12](#) describes QoS commands.

Table 4-12: QoS Commands

Command	Description
show qosprofile {<qosname> all}	Displays QoS profile information, including the following: <ul style="list-style-type: none"> ■ QoS profile name ■ Minimum bandwidth ■ Maximum bandwidth ■ Priority ■ The traffic groupings to which this profile is applied.

Table 4-12: QoS Commands (continued)

Command	Description
<code>config qosmode [explicit implicit]</code>	Changes the QoS mode to explicit mode or implicit mode.
<code>create qosprofile <qosname></code>	Creates a QoS profile. The default values assigned to a created QoS profile are as follows: <ul style="list-style-type: none"> ■ Minimum bandwidth — 0% ■ Maximum bandwidth — 100% ■ Priority — low
<code>delete qosprofile <qosname></code>	Deletes a QoS profile.
<code>config qosprofile <qosname> {minbw <percent>} {maxbw <percent>} {priority <level>}</code>	Configures a QoS profile. Specify: <ul style="list-style-type: none"> ■ <code>minbw</code> — The minimum bandwidth percentage guaranteed to be available to this queue. The default setting is 0. ■ <code>maxbw</code> — The maximum bandwidth percentage that this queue is permitted to use. The default setting is 100. ■ <code>priority</code> — The service priority for this queue. Settings include low, medium-low, medium, high. The default setting is low.

BASIC IP COMMANDS

[Table 4-13](#) describes basic IP commands.

Table 4-13: Basic IP Commands

Command	Description
<code>show ip config {vlan [<name> all]}</code>	Displays configuration information for one or more VLANs, including the following: <ul style="list-style-type: none"> ■ IP address, subnet mask ■ IP forwarding information ■ BOOTP configuration ■ VLAN name, VLANid

Table 4-13: Basic IP Commands (continued)

Command	Description
show ip stats {vlan [<name> all]}	Displays statistics of packets handled by the CPU, including the following: <ul style="list-style-type: none"> ■ inpackets, outpackets ■ ICMP/IGMP statistics ■ IRDP statistics
show ipfdb {<ipaddress> <netmask> vlan <name> all}	Displays the contents of the IP forwarding database table. Use for technical support purposes.
clear ipfdb [<ipaddress> <netmask> vlan <name> all]	Clears the dynamic entries in the IP forwarding database table.
enable ipforwarding {vlan <name> all}	Enables IP forwarding to an IP interface. If <code>all</code> is specified, then all the configured IP interfaces are affected. If no optional argument is provided, the <code>all</code> is assumed. Other IP configuration is not affected. When new IP interfaces are added, the interface is configured to have <code>ipforwarding</code> disabled by default.
disable ipforwarding {vlan <name> all}	Disables IP forwarding on one or all IP interfaces.
enable ipforwarding broadcast {vlan <name> all}	Enables forwarding of IP broadcast traffic on an IP interface. If <code>all</code> is specified, then all the configured IP interfaces are affected. If no optional argument is provided, then <code>all</code> is assumed. Other IP configuration is not affected. When new IP interfaces are added, the default is to have broadcast enabled.
disable ipforwarding broadcast {vlan <name> all}	Disables IP broadcast forwarding on one or all IP interfaces.
enable bootp vlan [<name> all]	Enables the generation and processing of BOOTP packets on a VLAN. The default setting is enabled for all VLANs.
disable bootp vlan [<name> all]	Disables the generation and processing of BOOTP packets.
enable bootprelay	Enables the BOOTP relay function on the router.
disable bootprelay	Disables the BOOTP relay function on the router.

Table 4-13: Basic IP Commands (continued)

Command	Description
config bootprelay add <ipaddress>	Adds IP addresses to be used as IP destinations to forward BOOTP packets.
config bootprelay delete [<ipaddress> all]	Deletes one or all IP addresses that were used as IP destinations to forward BOOTP packets.
show iparp {<ipaddress> vlan <name> all permanent}	Displays the current Address Resolution Protocol (ARP) cache for a selected IP address, VLAN, or all entries. With no options, information for all VLANs is displayed. Information displayed includes IP address, MAC address, aging timer value, VLAN name, VLANid, and port number.
clear iparp [<ipaddress> vlan <name> all]	Removes dynamic entries in the IP ARP table.
show iproute vlan {<name> all permanent}	Displays the contents of the IP routing table.
config iproute add default <gateway> {<metric>}	Adds a default gateway. A default gateway must be located on a configured IP interface.
config iproute delete default <gateway>	Deletes a default gateway.

IP ARP COMMANDS

[Table 4-14](#) describes IP ARP commands.

Table 4-14: IP ARP Commands

Command	Description
show iparp {<ipaddress> vlan <name> all permanent}	Displays the current Address Resolution Protocol (ARP) cache for a selected IP address, VLAN, or all entries. With no options, information for all VLANs is displayed. Information displayed includes IP address, MAC address, aging timer value, VLAN name, VLANid, and port number.
clear iparp [<ipaddress> vlan <name> all]	Removes dynamic entries in the IP ARP table.
config iparp add <ipaddress> <mac_address>	Adds a permanent IP ARP entry to the system. The IP address is used to match the IP interface address to locate a suitable interface.
config iparp delete <ipaddress>	Removes an IP ARP entry from the table.
show iproute vlan {<name> all permanent}	Displays the contents of the IP routing table.

Table 4-14: IP ARP Commands (continued)

Command	Description
config iproute add default <gateway> {<metric>}	Adds a default gateway. A default gateway must be located on a configured IP interface.
config iproute delete default <gateway>	Deletes a default gateway.

IP ROUTE TABLE COMMANDS

[Table 4-15](#) describes IP Route Table commands.

Table 4-15: IP Route Table Commands

Command	Description
show iproute vlan {<name> all permanent <ipaddress> <netmask>}	Displays the contents of the IP routing table.
config iproute add default <gateway> {<metric>}	Adds a default gateway to the routing table. A default gateway must be located on a configured IP interface . If no metric is specified, the default metric of 1 is used.
config iproute delete default <gateway>	Deletes a default gateway.
config iproute add <ipaddress> <mask> <gateway> {<metric>}	Adds a static address to the routing table. Use a value of 255.255.255.255 for <code>mask</code> to indicate a host entry.
config iproute delete <ipaddress> <mask> <gateway>	Deletes a static address from the routing table.
config iproute add blackhole <ipaddress> <mask>	Adds a <code>blackhole</code> address to the routing table. All traffic destined for the configured IP address is dropped, and no Internet Control Message Protocol (ICMP) message is generated.
config iproute delete blackhole <ipaddress> <mask>	Deletes a <code>blackhole</code> address from the routing table.

ICMP COMMANDS

Table 4-16 describes the commands used to configure the ICMP protocol.

Table 4-16: ICMP Commands

Command	Description
enable icmp redirects {vlan <name> all}	Enables generation of ICMP redirect messages on one or more VLANs. The default setting is enabled.
disable icmp redirects {vlan <name> all}	Disables the generation of ICMP redirects on one or more VLANs.
enable icmp unreachable {vlan <name> all}	Enables the generation of ICMP unreachable messages on one or more VLANs. The default setting is enabled.
disable icmp unreachable	Disables the generation of ICMP unreachable messages on one or more VLANs.
enable icmp userredirects	Enables the modification of route table information when an ICMP redirect message is received. The default setting is disabled.
disable icmp userredirects	Disables the changing of routing table information when an ICMP redirect message is received.
enable irdp {vlan <name> all}	Enables the generation of ICMP router advertisement messages on one or more VLANs. The default setting is enabled.
disable irdp {vlan <name> all}	Disables the generation of router advertisement messages on one or more VLANs.
config irdp [multicast broadcast]	Configures the destination address of the router advertisement messages. The default setting is broadcast.

Table 4-16: ICMP Commands (continued)

Command	Description
config irdp <mininterval> <maxinterval> <lifetime> <preference>	Configures the router advertisement message timers, using seconds. Specify: <ul style="list-style-type: none"> ■ <code>mininterval</code> — The minimum amount of time between router advertisements. The default setting is 450 seconds. ■ <code>maxinterval</code> — The maximum time between router advertisements. The default setting is 600 seconds. ■ <code>lifetime</code> — The default setting is 1,800 seconds. ■ <code>preference</code>
unconfig icmp	Resets all ICMP settings to the default values.
unconfig irdp	Resets all router advertisement settings to the default values.
disable irdp {vlan <name> all}	Disables the generation of router advertisement messages on one or more VLANs.

RIP COMMANDS

[Table 4-17](#) describes the commands used to configure the RIP protocol.

Table 4-17: RIP Commands

Command	Description
show rip {vlan <name> all}	Displays RIP configuration and statistics for one or more VLANs. Display includes the state for RIP settings, and interface states. Statistics include the following: <ul style="list-style-type: none"> ■ Packets transmitted ■ Packets received ■ Bad packets received ■ Bad routes received ■ Number of RIP peers ■ Peer information

Table 4-17: RIP Commands (continued)

Command	Description
	Displays RIP-specific statistics. Statistics include the following per interface: <ul style="list-style-type: none"> ■ Packets transmitted ■ Packets received ■ Bad packets received ■ Bad routes received ■ Number of RIP peers ■ Peer information
enable rip	Enables RIP.
disable rip	Disables RIP.
config rip add {vlan <name> all}	Configures RIP on an IP interface. If no VLAN is specified, then <code>all</code> is assumed. When an IP interface is created, per interface RIP configuration is enabled by default.
config rip delete {vlan <name> all}	Disables RIP on an IP interface. When RIP is disabled on the interface, the parameters are not reset to their defaults.
enable rip aggregation	Enables RIP aggregation of subnet information on a RIP version 2 interface. The default setting is enabled.
disable rip aggregation	Disables the RIP aggregation of subnet information on a RIP version 2 interface.
enable rip splithorizon	Enables the split horizon algorithm for RIP. Default setting is enabled.
disable rip splithorizon	Disables split horizon.
enable rippoisonreverse	Enables the split horizon with poison-reverse algorithm for RIP. The default setting is enabled.
disable rip poisonreverse	Disables poison reverse.
enable rip triggerupdate	Enables triggered updates. <i>Triggered updates</i> are a mechanism for immediately notifying a router's neighbors when the router adds or deletes routes, or changes the metric of a route. The default setting is enabled.
disable rip triggerupdate	Disables triggered updates.
enable rip exportstatic	Enables the advertisement of static routes using RIP. The default setting is enabled.

Table 4-17: RIP Commands (continued)

Command	Description
<code>disable rip exportstatic</code>	Disables the filtering of static routes.
<code>config rip updatetime {<delay>}</code>	Changes the periodic RIP update timer. The default setting is 30 seconds.
<code>config rip routetimeout {<delay>}</code>	Configures the route timeout. The default setting is 180 seconds.
<code>config rip garbagetime {<delay>}</code>	Configures the RIP garbage time. The default setting is 120 seconds.
<code>config rip txmode [none v1only v1comp v2only] {vlan <name> all}</code>	<p>Changes the RIP transmission mode for one or more VLANs. Specify:</p> <ul style="list-style-type: none"> ■ <code>none</code> — Do not transmit any packets on this interface. ■ <code>v1only</code> — Transmit RIP version 1 format packets to the broadcast address. ■ <code>v1comp</code> — Transmit version 2 format packets to the broadcast address. ■ <code>v2only</code> — Transmit version 2 format packets to the RIP multicast address. <p>If no VLAN is specified, the setting is applied to all VLANs. The default setting is <code>v2only</code>.</p>
<code>config rip rxmode [none v1only v2only any] {vlan <name> all}</code>	<p>Changes the RIP receive mode for one or more VLANs. Specify:</p> <ul style="list-style-type: none"> ■ <code>none</code> — Drop all received RIP packets. ■ <code>v1only</code> — Accept only RIP version 1 format packets. ■ <code>v2only</code> — Accept only RIP version 2 format packets. ■ <code>any</code> — Accept both version 1 and version 2 packets. <p>If no VLAN is specified, the setting is applied to all VLANs. The default setting is <code>any</code>.</p>
<code>unconfig rip {vlan <name> all}</code>	Resets all RIP parameters to the default VLAN. Does not change the enable/disable state of the RIP settings.

LOGGING COMMANDS

Table 4-18 describes Switch logging commands.

Table 4-18: Logging Commands

Command	Description
show log config	Displays the log configuration, including the syslog host IP address, the priority level of messages being logged locally, and the priority level of messages being sent to the syslog host.
show log {<priority>} {<subsystem>}	<p>Displays the current snapshot of the log. Options include:</p> <ul style="list-style-type: none"> ■ priority — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed. ■ subsystem — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP, Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.
clear log	Clears the log.
config log display {<priority>} {<subsystem>}	<p>Configures the real-time log display. Options include:</p> <ul style="list-style-type: none"> ■ priority — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed. ■ subsystem — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.

Table 4-18: Logging Commands (continued)

Command	Description
config syslog <ipaddress> <facility> {<priority>} {<subsystem>}	Configures the syslog host address and filter messages sent to the syslog host. Options include: <ul style="list-style-type: none"> ■ ipaddress — The IP address of the syslog host. ■ facility — The syslog facility level for local use. ■ priority — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, only critical priority messages are sent to the syslog host. ■ subsystem — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are sent to the syslog host.
enable log display	Enables the log display.
disable log display	Disables the log display.
enable syslog	Enables logging to a remote syslog host.
disable syslog	Disables logging to a remote syslog host.

CONFIGURATION AND IMAGE COMMANDS

[Table 4-19](#) describes configuration and image commands

Table 4-19: Configuration and Image Commands

Command	Description
save {config} {primary secondary}	Downloads a previously saved ASCII configuration file from a specific IP host. You must specify the IP address of the host and the configuration filename.

Table 4-19: Configuration and Image Commands (continued)

Command	Description
use config {primary secondary}	Configures the Switch to use a particular configuration on the next reboot. Options include the primary configuration area, or the secondary configuration area. If not specified, the Switch will use the primary configuration area.
use image {primary secondary}	Configures the Switch to use a particular image on the next reboot. If not specified, the Switch will use the primary image.
download image <ipaddress> <filename> {primary secondary}	Downloads a new image from a TFTP server. You must specify the IP address of the TFTP server and the image filename. You can optionally specify if you want the file downloaded to the primary or secondary image. If you do not specify, the file is downloaded to the primary image.

5

Virtual LANs (VLANs)

Setting up Virtual Local Area Networks (VLANs) on the Summit eases many time-consuming tasks of network administration while increasing efficiency in network operations.

This chapter describes the concept of VLANs and explains how to implement VLANs on the Summit.

OVERVIEW OF VIRTUAL LANs

The term VLAN is used to refer to a collection of devices that communicate as if they were on the same physical LAN. Any set of ports (including all ports on the Switch) is considered a VLAN. LAN segments are not restricted by the hardware that physically connects them. The segments are defined by flexible user groups you create with the command-line interface.

BENEFITS

Implementing VLANs on your networks has the following advantages:

- **VLANs help to control traffic.**

With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether they require it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that must communicate with each other.

- **VLANs provide extra security.**

Devices within each VLAN can only communicate with member devices in the same VLAN. If a device in VLAN *Marketing* must communicate with devices in VLAN *Sales*, the traffic must cross a routing device.

- **VLANs ease the change and movement of devices.**

With traditional networks, network administrators spend much of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each endstation must be updated manually.

For example, with a VLAN, if an endstation in VLAN *Marketing* is moved to a port in another part of the network, and retains its original subnet membership; you must only specify that the new port is in VLAN *Marketing*.

TYPES OF VLANs

The Summit supports a maximum of 256 VLANs. Summit VLANs can be created according to the following criteria:

- Physical port
- 802.1Q tag
- Ethernet protocol type
- A combination of these criteria

PORT-BASED VLANs

In a port-based VLAN, a VLAN name is given to a group of one or more ports on the Switch. A Switch port can be a member of only one port-based VLAN.

For example, in [Figure 5-1](#), ports 1, 2, and 5 are part of VLAN *Marketing*; ports 3, 4, and 6 are part of VLAN *Sales*; and ports 7 and 8 are in VLAN *Finance*.

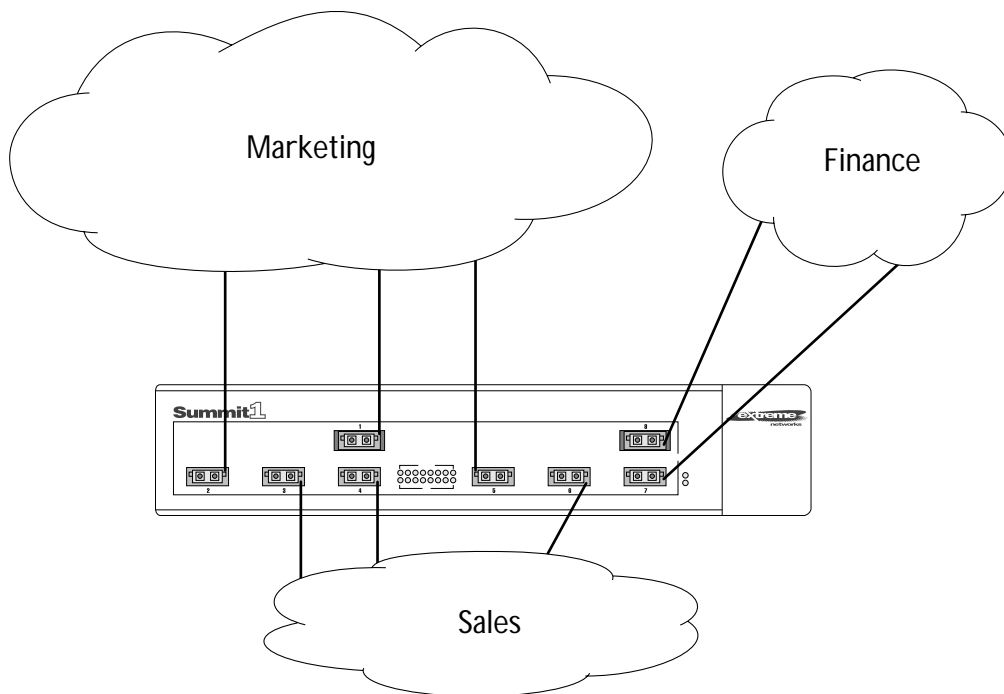


Figure 5-1: Example of a port-based VLAN

Even though they are physically connected to the same Switch, for the members of the different VLANs to communicate, the traffic must go through the IP routing functionality provided in the Summit. This means that each VLAN must be configured as a router interface with a unique IP address.

SPANNING SWITCHES WITH PORT-BASED VLANS

To create a port-based VLAN that spans two Switches, you must do two things:

- Assign the port on each Switch to the VLAN.
- Cable the two Switches together using one port on each Switch per VLAN.

Figure 5-2: illustrates a single VLAN that spans two Switches. All ports on both Switches belong to VLAN *Sales*. The two Switches are connected using port 2 on Switch 1, and port 6 on Switch 2.

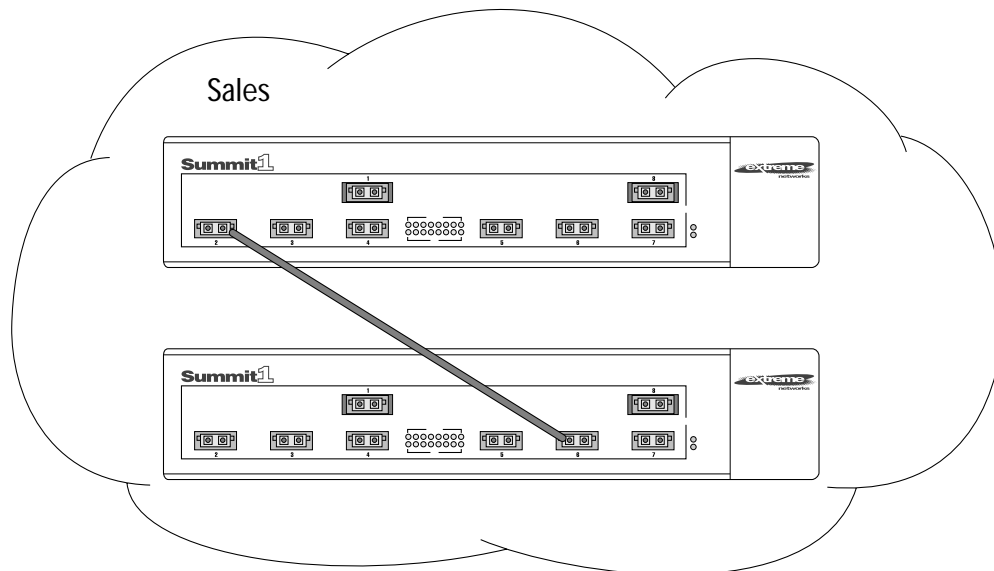


Figure 5-2: Single port-based VLAN spanning two Switches

In a port-based VLAN, to create multiple VLANs that span two Switches, a port on Switch 1 must be cabled to a port on Switch 2 for each VLAN you want to create. At least one port on each switch must be a member of one of the VLANs, as well.

Figure 5-3 illustrates two VLANs spanning two Switches. On Switch 1, ports 1-4 are part of VLAN *Accounting*; ports 5 - 8 are part of VLAN *Engineering*. On Switch 2, ports 1-4 are part of VLAN *Accounting*; ports 5 - 8 are part of VLAN *Engineering*. VLAN *Accounting* spans Switch 1 and Switch 2 by way of a connection between Switch 1 port 2 and Switch 2 port 4. VLAN *Engineering* spans Switch 1 and Switch 2 by way of a connection between Switch 1 port 5 and Switch 2 port 8.

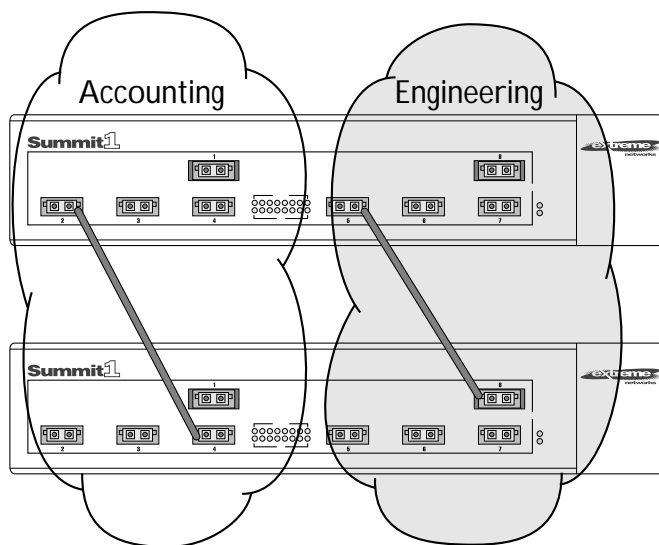


Figure 5-3: Two port-based VLANs spanning two Switches

Using these steps, you can create multiple VLANs that span multiple Switches, in a daisy-chained fashion. Each Switch must have a dedicated port for each VLAN. Each dedicated port must be connected to a port that is a member its VLAN on the next Switch.

TAGGED VLANs

Tagging is a process that inserts a marker (called a *tag*) into the Ethernet frame. The tag contains the identification number of a specific VLAN, called the *VLAN ID*.



The use of 802.1Q tagged packets may lead to the appearance of packets slightly bigger than the current IEEE 802.3/Ethernet maximum of 1518 bytes. This may affect packet error counters in other devices, and may also lead to connectivity problems if non-802.1Q bridges or routers are placed in the path.

USES OF TAGGED VLANs

Tagging is most commonly used to create VLANs that span Switches. The Switch-to-Switch connections are typically called *trunks*. Using tags, multiple VLANs can span multiple Switches using one or more trunks. In a port-based VLAN, each VLAN requires its own pair of trunk ports, as shown in [Figure 5-3](#). Using tags, multiple VLANs can span two Switches with a single trunk.

Another benefit of tagged VLANs is the ability to have a port be a member of multiple VLANs. This is particularly useful if you have a device (such as a server) that must belong to multiple VLANs. The device must have a NIC that supports 802.1Q tagging.

A single port can be a member of only one port-based VLAN. All additional VLAN membership for the port must be accompanied by tags. In addition to configuring the VLAN tag for the port, the server must have a *Network Interface Card (NIC)* that supports 802.1Q tagging.

ASSIGNING A VLAN TAG

Each VLAN may be assigned an 802.1Q VLAN tag. As ports are added to a VLAN with an 802.1Q tag defined, you decide whether each port will use tagging for that VLAN. The default mode of the Switch is to have all ports assigned to the VLAN named “default,” without an 802.1Q VLAN tag (VLAN ID) assigned.

Not all ports in the VLAN must be tagged. As traffic from a port is forwarded out of the Switch, the Switch determines (in real time) if each destination port should use tagged or untagged packet formats for that VLAN. The Switch adds and strips tags, as required, by the port configuration for that VLAN.



Packets arriving tagged with a VLAN ID that is not configured in the Switch will be discarded.

Figure 5-4 illustrates the physical view of a network that uses tagged and untagged traffic.

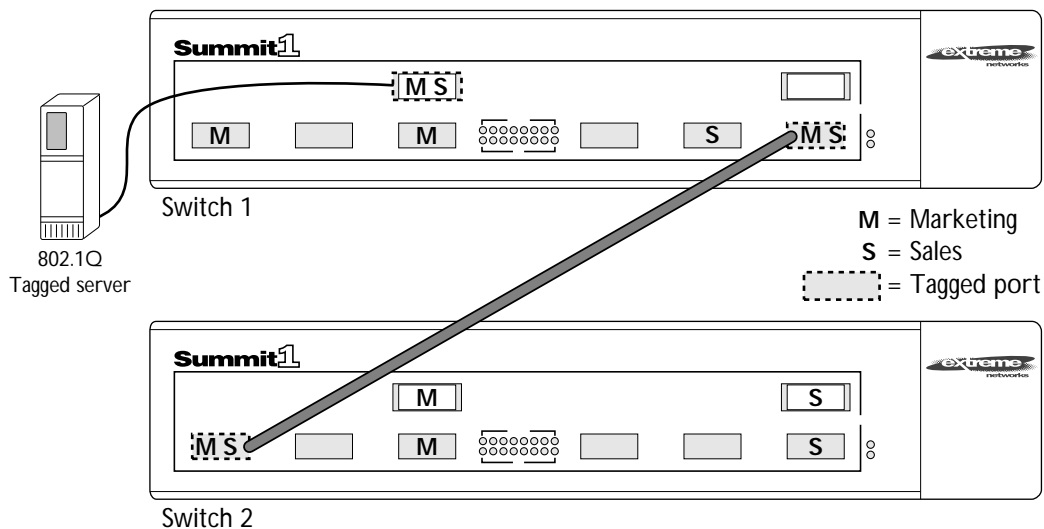


Figure 5-4: Physical diagram of tagged and untagged traffic

Figure 5-5 shows a logical diagram of the same network.

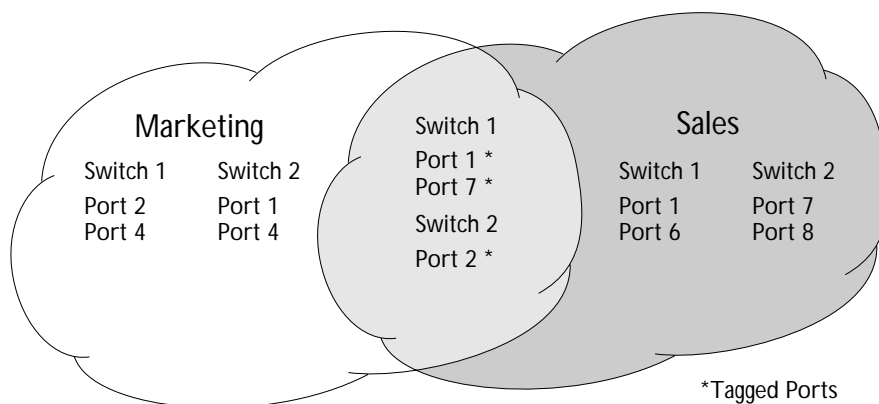


Figure 5-5: Logical diagram of tagged and untagged traffic

In [Figure 5-4](#) and [Figure 5-5](#):

- The trunk port on each Switch carries traffic for both VLAN *Marketing* and VLAN *Sales*.
- The trunk port on each Switch is tagged.
- The server connected to port 1 on Switch 1 has a NIC that supports 802.1Q tagging.
- The server connected to port 1 on Switch 1 is a member of both VLAN *Marketing* and VLAN *Sales*.
- All other stations use untagged traffic.

As data passes out of the Switch, the Switch determines if the destination port requires the frames to be tagged or untagged. All traffic coming from and going to the server is tagged. Traffic coming from and going to the trunk ports is tagged. The traffic that comes from and goes to the other stations on this network is not tagged.

MIXING PORT-BASED AND TAGGED VLANs

You can configure the Summit using a combination of port-based and tagged VLANs. A given port can be a member of multiple VLANs, with the stipulation that only one of its VLANs uses untagged traffic. In other words, a port can simultaneously be a member of one port-based VLAN and multiple tag-based VLANs.



For the purposes of VLAN classification, packets arriving on a port with an 802.1Q tag containing a VLAN ID of zero are treated as untagged.

PROTOCOL-BASED VLANs

Protocol-based VLANs enable you to define a packet filter that the Summit uses as the matching criteria to determine if a particular packet belongs to a particular VLAN.

Protocol-based VLANs are most often used in situations where network segments contain hosts running multiple protocols. For example, in [Figure 5-6](#), the hosts are running both the IP and NetBIOS protocols.

The IP traffic has been divided into two IP subnets, 192.207.35.0 and 192.207.36.0. The subnets are internally routed by the Summit. The subnets are assigned different VLAN names, *Finance* and *Personnel*, respectively. The remainder of the traffic belongs to the VLAN named *MyCompany*. All ports are members of the VLAN *MyCompany*.

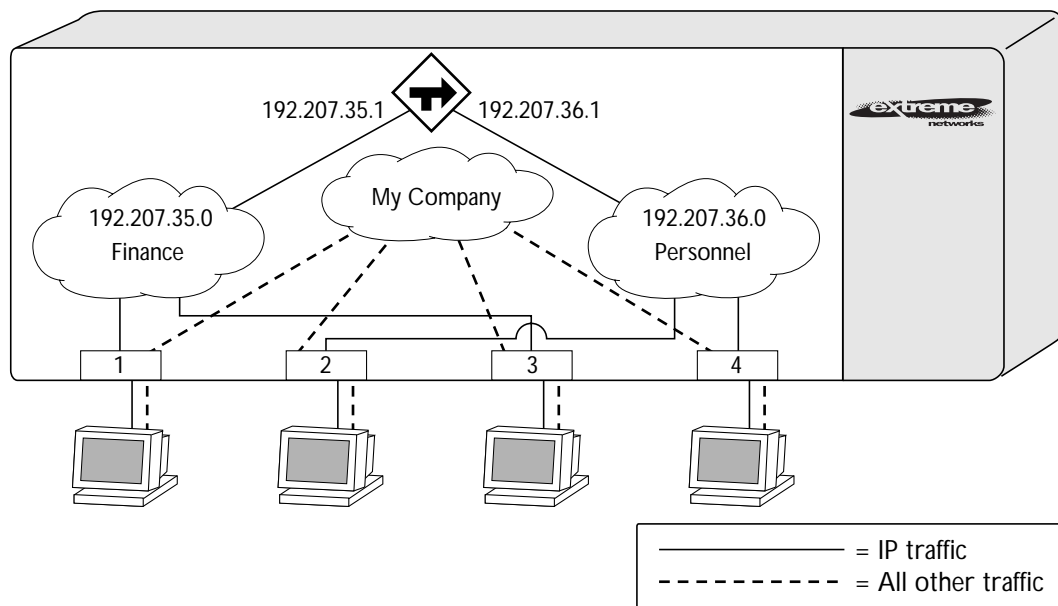


Figure 5-6: Protocol-based VLANs

PREDEFINED PROTOCOL FILTERS

The following protocol filters are predefined on the Summit:

- IP
- IPX
- NetBIOS
- DECNet

DEFINING PROTOCOL FILTERS

If necessary, you can define a customized protocol filter based on EtherType, LLC, and/or SNAP. Up to six filters may be part of a protocol filter. To define a protocol filter, do the following:

- Create a protocol using the following command:

```
create protocol <protocol_name>
```

- Configure the protocol using the following command:

```
config protocol <protocol_name> add <protocol_type> <hex_value>
```

Supported protocol types include:

- EtherType
- LLC
- SNAP

A maximum of seven protocol names, each containing a maximum of six protocol filters, can be defined.

VLAN NAMES

The Summit supports up to 256 different VLANs. Each VLAN is given a name that can be up to 32 characters. VLAN names can use standard alphanumeric characters. The following characters are not permitted in a VLAN name:

- Space
- Comma
- Quotation mark

VLAN names must begin with an alphabetical letter. Quotation marks can be used to enclose a VLAN name that does not begin with an alphabetical character, or that contains a space, comma, or other special character.

VLAN names are locally significant. That is, VLAN names used on one Switch are only meaningful to that Switch. If another Switch is connected to it, the VLAN names have no significance to the other Switch.

DEFAULT VLAN

The Summit ships with one default VLAN that has the following properties:

- The VLAN name is *default*.
- It contains all the ports on a new or initialized Switch.
- The default VLAN is untagged on all ports. It has an internal VLAN ID of 1.

CONFIGURING VLANs ON THE SUMMIT

This section describes the commands associated with setting up VLANs on the Summit. Configuring a VLAN involves the following steps:

- 1 Create and name the VLAN.
- 2 Assign an IP address and mask (if applicable) to the VLAN, if needed.
- 3 Assign a VLAN ID, if any ports in this VLAN will use a tag.
- 4 Assign one or more ports to the VLAN.

As you add each port to the VLAN, decide if the port will use an 802.1Q tag.

[Table 5-1](#) describes the commands used to configure a VLAN.

Table 5-1: VLAN Configuration Commands

Command	Description
create vlan <name>	Creates a named VLAN.
create protocol <protocol_name>	Creates a user-defined protocol.
config dot1p ethertype <ethertype>	Configures an IEEE 802.1Q Ethertype. Use this command only if you have another Switch that supports 802.1Q, but uses a different Ethertype value than 8100.
config protocol <protocol_name> [add delete] <prototype_number> {<prototype_number>} ...	Configures a protocol filter. Supported protocol types include: <ul style="list-style-type: none"> ■ EtherType ■ LLC ■ SNAP
config vlan <name> ipaddress <ipaddress> {<mask>}	Assigns an IP address and an optional mask to the VLAN.


Table 5-1: VLAN Configuration Commands (continued)

Command	Description
config vlan <name> [add delete] port <portlist> {tagged untagged}	Adds and deletes ports. You can specify tagged and untagged port(s). By default, ports are untagged.
config vlan <name> protocol [<protocol_name> any]	Configures a protocol-based VLAN. If the keyword <i>any</i> is specified, then it becomes the default VLAN. All packets that cannot be classified into other protocol-based VLANs are assigned to the default VLAN of that port.
config vlan <name> qosprofile <qosname>	Configures a VLAN to use a particular QoS profile. Dynamic FDB entries associated with the VLAN are flushed once the change is committed.
config vlan <name> tag <vlanid>	Assigns a numerical VLAN ID. The valid range is from 1 to 4095.

VLAN CONFIGURATION EXAMPLES

The following example creates a port-based VLAN named *accounting*, assigns the IP address 132.15.121.1, and assigns ports 1, 2, 3, and 6 to it:

```
create vlan accounting
config accounting ipaddress 132.15.121.1
config accounting add port 1-3,6
```

 *Because VLAN names are unique, you do not need to enter the keyword `vlan` after you have created the unique VLAN name. You can use the VLAN name alone.*

The following example creates a tag-based VLAN named *video*. It assigns the VLAN ID 1000. Ports 4 through 8 are added as tagged ports to the VLAN.

```
create vlan video
config video tag 1000
config video add port 4-8 tagged
```

The following example creates a VLAN named *Sales*, with the VLAN ID 120. The VLAN uses both tagged and untagged ports. Ports 1 through 3 are tagged, and ports 4 and 7 are untagged. Note that when not explicitly specified, ports are added as untagged.

```
create vlan sales
config sales tag 120
config sales add port 1-3 tagged
config sales add port 4,7
```

The following example creates a protocol-based vlan named *IPSales*. Ports 6 through 8 are assigned to the VLAN.

```
create vlan ipsales
config ipsales protocol ip
config ipsales add port 6-8
```

The following example defines a protocol filter, *myprotocol*, for the purposes of later applying to a VLAN. This is an example only, and has no real-world application.

```
create protocol myprotocol
config protocol myprotocol add etype 0xf0f0
config protocol myprotocol add etype 0xffff
```

DISPLAYING VLAN SETTINGS

To display VLAN settings, use the following command:

```
show vlan {<name> | all}
```

Sample output from this command is as follows:

```
show vlan all

      "Default", 802.1Q Tag 1, created by user.
      IP Address 0.0.0.0 netmask 0.0.0.0
      Member of Spanning Tree Domain s0
      Number of ports: 0

      VLAN does not contain any ports !
      Protocol=ANY = [EtherType=ffff]
```

```
"accounting", Untagged (Internal tag 4095), created by user.  
IP Address 192.208.37.13 netmask 255.255.255.0  
Member of Spanning Tree Domain s0  
Number of ports: 4
```

```
Configured untagged ports:  
  3 2 1 6
```

```
Protocol=ANY = [EtherType=ffff]
```

```
"video", 802.1Q Tag 100, created by user.  
Routing Information is not configured  
Member of Spanning Tree Domain s0  
Number of ports: 5
```

```
Configured tag ports:  
  4 5 6 7 8
```

```
Protocol=ANY = [EtherType=ffff]
```

The `show` command displays summary information about each VLAN, and includes the following:

- Name
- VLAN ID
- Ports assigned
- Tagged/untagged status for each port
- Protocol information
- IP address
- QOS profile information
- STPD information

To display protocol information, use the following command:

```
show protocol {<protocol> | all}
```

Sample output from this command is as follows.

```
show protocol all
```

Protocol Name	Type	Value
-----	----	-----
IP	etype	0x0806
	etype	0x0800
ipx	etype	0x8137
netbios	llc	0xf0f0
decnet	etype	0x6004
	etype	0x6003

This `show` command displays protocol information, including the following:

- Protocol name
- List of protocol fields
- VLANs that use the protocol

DELETING VLANs

To delete a VLAN, or to return VLAN settings to their defaults, use the commands listed in [Table 5-2](#).

Table 5-2: VLAN Delete and Reset Commands

Command	Description
unconfig vlan <name> ipaddress	Resets the IP address of the VLAN.
delete vlan <name>	Removes a VLAN.
delete protocol <protocol>	Removes a protocol.

6

Switch Forwarding Database (FDB)

This chapter describes contents of the the Switch forwarding database (FDB), how the FDB works, and how to configure the FDB.

OVERVIEW OF THE FDB

The Summit maintains a database of all media access control (MAC) addresses received on all of its ports. It uses the information in this database to decide whether a frame should be forwarded or filtered.

FDB CONTENTS

The database holds up to a maximum of 128K entries. Each entry consists of the MAC address of the device, an identifier for the port on which it was received, and an identifier for the VLAN to which the device belongs. Frames destined for devices that are not in the FDB are flooded to all members of the VLAN.

FDB ENTRY TYPES

The following are three types of entries in the FDB:

- **Dynamic entries** — Initially, all entries in the database are dynamic. Entries in the database are removed (aged-out) if, after a period of time (aging time), the device has not transmitted. This prevents the database from becoming full with obsolete entries by ensuring that when a device is removed from the network, its entry is deleted from the database. Dynamic entries are deleted from the database if the

Switch is reset or a power off/on cycle occurs. For more information about setting the aging time, refer to the section [“Configuring FDB Entries,”](#) later in this chapter.

- **Static entries** — If the aging time is set to zero, all aging entries in the database are defined as static, non-aging entries. This means that they do not age, but they are still deleted if the Switch is reset.
- **Permanent entries** — Permanent entries are retained in the database if the Switch is reset or a power off/on cycle occurs. The system administrator must make entries permanent. A permanent entry can either be a unicast or multicast MAC address. All entries entered by way of the command-line interface are stored as permanent. The Switch can support a maximum of 64 permanent entries.

HOW FDB ENTRIES GET ADDED

Entries are added into the FDB in two ways:

- The Switch can learn entries. The Switch updates its FDB with the source MAC address from a packet, the VLAN, and the port identifier on which the source packet is received.
- You can enter and update entries using a MIB browser, an SNMP Network Manager, or the command-line interface, as described in the next section.

CONFIGURING FDB ENTRIES

To configure entries in the FDB, use the commands listed in [Table 6-1](#).

Table 6-1: FDB Configuration Commands

Command	Description
create fdbentry <macaddress> vlan <name> <portlist> {qosprofile <qosname>}	<p>Creates a permanent FDB entry. Specify the following:</p> <ul style="list-style-type: none">■ <code>macaddress</code> — Device MAC address, using colon separated bytes.■ <code>name</code> — VLAN associated with MAC address.■ <code>portlist</code> — Port numbers associated with MAC address.■ <code>qosname</code> — QoS profile associated with MAC address. <p>If more than one port number is associated with a permanent MAC entry, packets are multicast to the multiple destinations.</p>

Table 6-1: FDB Configuration Commands (continued)

Command	Description
<code>config fdb agingtime <delay></code>	Configures the FDB aging time. The range is 15 through 1,000,000 seconds. The default value is 300 seconds. A value of 0 indicates that the entry should never be aged out.

FDB CONFIGURATION EXAMPLE

This example adds a permanent entry to the FDB:

```
create fdbentry 00:E0:2B:12:34:56 vlan marketing port 4
```

The permanent entry has the following characteristics:

- MAC address is 00E02B123456.
- VLAN name is *marketing*.
- Port number for this device is 4.

DISPLAYING FDB ENTRIES

To display FDB entries, use the command

```
show fdb {all | <macaddress> | vlan <name> | <portlist> | permanent}
```

where the following is true:

- `all` — Displays all FDB entries.
- `macaddress` — Displays the entry for a particular MAC address.
- `vlan <name>` — Displays the entries for a VLAN.
- `portlist` — Displays the entries for a port.
- `permanent` — Displays all permanent entries.

The following sample output shows the information displayed when you request output for all FDB entries:

```
show fdb

Hash Num Mac                               Vlan                               Flags  Ptag  PortList
-----
0ff0: 0  ff:ff:ff:ff:ff:ff  Default(0001)  sm    0fdf  CPU,1,19
1823: 0  08:00:4e:2b:f3:00  Default(0001)  sm    0ff1  CPU
2bfb: 0  00:80:c7:01:cb:bd  Default(0001)  dm    0000  1
3289: 0  00:e0:2b:00:00:00  Default(0001)  sm    0ffb  CPU
373d: 0  01:80:c2:00:00:00  (0000)        sm    0ffb  CPU

Total: 5 Static: 4 Perm: 0 Dyn: 1 Dropped: 0
FDB Aging time: 300 seconds
```

The `show` command displays summary information, including

- MAC address
- VLAN name and VLANid
- Entry method (dynamic/static/permanent)
- Port

REMOVING FDB ENTRIES

You can remove one or more specific entries from the FDB, or you can clear the entire FDB of all entries by using the commands listed in [Table 6-2](#).

Table 6-2: Removing FDB Entry Commands

Command	Description
<code>delete fdbentry <macaddress> vlan <name></code>	Deletes a permanent FDB entry.
<code>clear fdb {all <macaddress> vlan <name> <portlist>}</code>	Clears dynamic FDB entries that match the filter. Use the keyword <code>all</code> to clear all dynamic entries.

7

Spanning Tree Protocol (STP)

Using the Spanning Tree Protocol (STP) functionality of the Summit makes your network more fault tolerant.

The following sections explain more about STP and the STP features supported by the Switch.



STP is a part of the 802.1D bridge specification defined by the IEEE Computer Society. To explain STP in terms used by the 802.1D specification, the Summit will be referred to as a bridge.

OVERVIEW OF THE SPANNING TREE PROTOCOL

STP is a bridge-based mechanism for providing fault tolerance on networks. STP allows you to implement parallel paths for network traffic, and ensure that

- Redundant paths are disabled when the main paths are operational.
- Redundant paths are enabled if the main path fails.

SPANNING TREE DOMAINS

The Summit can be partitioned into multiple virtual bridges. Each virtual bridge can run an independent Spanning Tree instance. Each Spanning Tree instance is called a *Spanning Tree Domain* (STPD). Each STPD has its own Root Bridge and active path. Once the STPD is created, one or more VLANs can be assigned to it.

A port can belong to only one STPD. If a port is a member of multiple VLANs, then all those VLANs must belong to the same STPD.

The key points to remember when configuring VLANs and STP are the following:

- Each VLAN forms an independent broadcast domain.
- STP blocks paths to create a loop-free environment.
- When STP blocks a path, no data can be transmitted or received on the blocked port.
- Within any given STPD, all VLANs belonging to it use the same spanning tree.



Care must be taken to ensure that STPD instances within a single Summit Switch do not see each other in the same broadcast domain. This could happen if, for example, another external bridge is used to connect VLANs belonging to separate STPDs.

DEFAULTS

The default device configuration contains a single STPD called *s0*. The default VLAN is a member of STPD *s0*.

All STP parameters default to the IEEE 802.1D values, as appropriate.

STP CONFIGURATIONS

When you assign VLANs to an STPD, pay careful attention to the STP configuration and its effect on the forwarding of VLAN traffic.

[Figure 7-1](#) illustrates a network that uses VLAN tagging for trunk connections. The following four VLANs have been defined:

- *Sales* is defined on Switch A, Switch B, and Switch M.
- *Personnel* is defined on Switch A, Switch B, and Switch M.
- *Manufacturing* is defined on Switch Y, Switch Z, and Switch M.
- *Engineering* is defined on Switch Y, Switch Z, and Switch M.
- *Marketing* is defined on all Switches (Switch A, Switch B, Switch Y, Switch Z, and Switch M).

Two STPDs are defined:

- STPD1 contains VLANs *Sales* and *Personnel*.
- STPD2 contains VLANs *Manufacturing* and *Engineering*.

The VLAN *Marketing* is not assigned to a STPD.

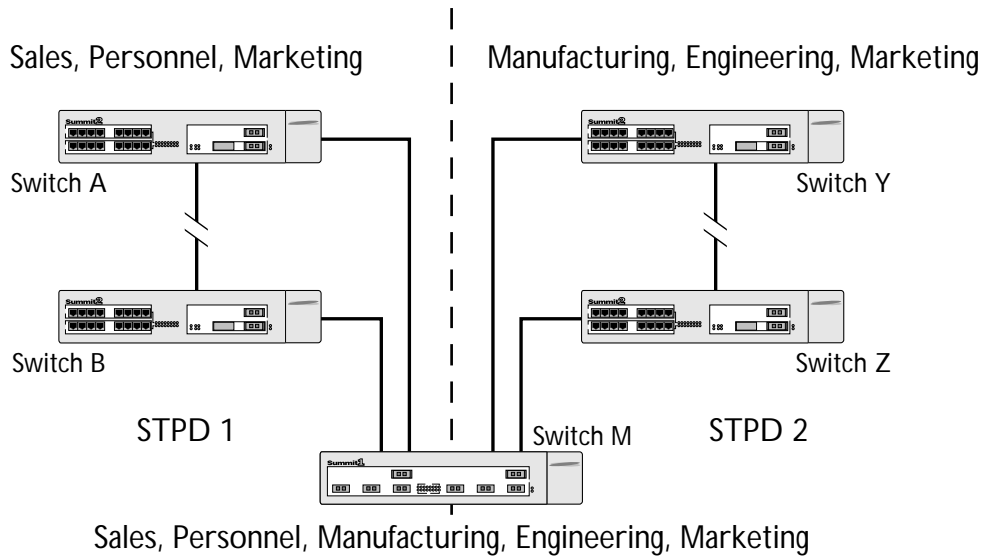


Figure 7-1: Multiple Spanning Tree Domains

When this configuration's Switches start up, STP configures each STP domain such that there are no active loops in the topology. STP could configure the topology in a number of ways to make it loop-free.

In [Figure 7-1](#), the connection between Switch A and Switch B is put into blocking state, and the connection between Switch Y and Switch Z is put into blocking state. After STP converges, all the VLANs can communicate, and all bridging loops are prevented.

The VLAN *Marketing*, which has not been assigned to any STPD, communicates using all five Switches. The topology has no loops, because STP has already blocked the port connection between Switch A and Switch B, and between Switch Y and Switch Z.

Within a single STPD, you must be extra careful when configuring your VLANs.

Figure 7-2 illustrates a network that has been incorrectly set up using a single STPD so that the STP configuration disables the ability of the Switches to forward VLAN traffic.

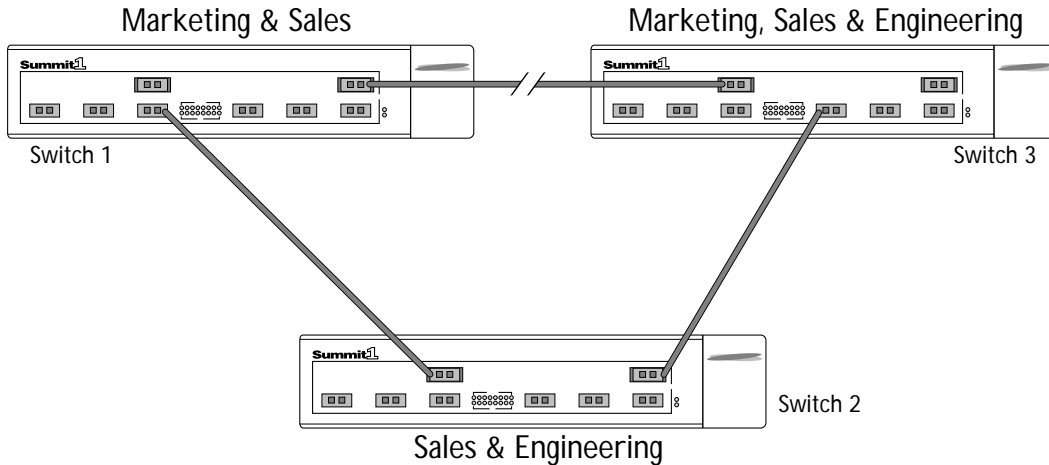


Figure 7-2: Tag-based STP configuration

The tag-based network in Figure 7-2 has the following configuration:

- Switch 1 contains VLAN *Marketing* and VLAN *Sales*.
- Switch 2 contains VLAN *Engineering* and VLAN *Sales*.
- Switch 3 contains VLAN *Marketing*, VLAN *Engineering*, and VLAN *Sales*.
- The tagged trunk connections for three Switches form a triangular loop that is not permitted in an STP topology.
- All VLANs in each Switch are members of the same STPD.

STP may block traffic between Switch 1 and Switch 3 by disabling the trunk ports for that connection on each Switch.

Switch 2 has no ports assigned to VLAN *marketing*. Therefore, if the trunk for VLAN *marketing* on Switches 1 and 3 is blocked, the traffic for VLAN *marketing* will not be able to traverse the Switches.

CONFIGURING STP ON THE SUMMIT

STP configuration involves the following actions:

- Create one or more STP domains using the following command:

```
create stpd <stpd_name>
```



STPD, VLAN, and QoS profile names must all be unique. For example, a name used to identify a VLAN cannot be used when you create an STPD or a QoS profile.

- Add one or more VLANs to the STPD using the following command:

```
config stpd <stpd_name> add vlan <name>
```

- Enable STP for one or more STP domains using the following command:

```
enable stpd [<stpd_name> | all]
```

Once you have created the STPD, you can optionally configure STP parameters for the STPD.



You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

The following parameters can be configured on each STPD:

- Hello time
- Forward delay
- Max age
- Bridge priority

The following parameters can be configured on each port:

- Path cost
- Port priority



The device supports the RFC 1493 Bridge MIB. Parameters of only the s0 default STPD are accessible through this MIB.

Table 7-1 shows the commands used to configure STP.

Table 7-1: STP Configuration Commands

Command	Description
create stpd <stpd_name>	Creates an STPD. When created, an STPD has the following default parameters: <ul style="list-style-type: none"> ■ Bridge priority — 32,768 ■ Hello time — 2 seconds ■ Forward delay — 15 seconds
enable stpd [<stpd_name> all]	Enables the STP protocol for one or all STPDs. The default setting is disabled.
enable stpd port <portlist>	Enables the STP protocol on one or more ports. If STPD is enabled for a port, BPDUs will be generated on that port if STP is enabled for the associated STPD. The default setting is enabled.
config stpd <stpd_name> add vlan <name>	Adds a VLAN to the STPD.
config stpd <stpd_name> delete vlan [<name> all]	Removes one or all VLANs from an STPD. If all is specified, the association between the STPD and VLAN is removed, but both are still instantiated.
config stpd <stpd_name> hellotime <value>	Specifies the time delay (in seconds) between the transmission of BPDUs from this STPD when it is the Root Bridge. The range is 1 through 10. The default setting is 2 seconds.
config stpd <stpd_name> forwarddelay <value>	Specifies the time (in seconds) that the ports in this STPD spend in the listening and learning states when the Switch is the Root Bridge. The range is 4 through 30. The default setting is 15 seconds.
config stpd <stpd_name> maxage <value>	Specifies the maximum age of a BPDU in this STPD. The range is 6 through 40. The default setting is 20 seconds. Note that the time must be greater than, or equal to 2 X (Hello Time + 1) and less than, or equal to 2 X (Forward Delay -1).

Table 7-1: STP Configuration Commands (continued)

Command	Description
config stpd <stpd_name> priority <value>	<p>Specifies the priority of the STPD. By changing the priority of the STPD, you can make it more or less likely to become the Root Bridge.</p> <p>The range is 0 through 65,535. The default setting is 32,768. A setting of 0 indicates the highest priority.</p>
config stpd <stpd_name> port cost <value> <portlist>	<p>Specifies the path cost of the port in this STPD.</p> <p>The range is 1 through 65,535. The Switch automatically assigns a default path cost based on the speed of the port, as follows:</p> <ul style="list-style-type: none">■ For a 10Mbps port, the default cost is 100.■ For a 100Mbps port, the default cost is 19.■ For a 1000Mbps port, the default cost is 4.
config stpd <stpd_name> port priority <value> <portlist>	<p>Specifies the priority of the port in this STPD. By changing the priority of the port, you can make it more or less likely to become the Root Port.</p> <p>The range is 0 through 255. The default setting is 128. A setting of 0 indicates the lowest priority.</p>

CONFIGURATION EXAMPLE

The following example creates and enables an STPD named *Backbone_st*. It assigns the *Manufacturing* VLAN to the STPD. It disables STP on ports 1 through 7, and port 12.

```
create stpd backbone_st
config stpd backbone_st add vlan manufacturing
enable stpd backbone_st
disable stpd backbone_st port 1-7,12
```

DISPLAYING STP SETTINGS

To display STP settings for all ports, use the following command:

```
show stpd {<stpd_name> | all}
```

This command displays the following information:

- STPD name
- Bridge ID
- STPD configuration information

Sample output from the command is as follows:

```
show stpd
```

```
Stpd:s0                      Stp:DISABLED          Number of Ports:8
Ports: 1,2,3,4,5,6,7,8
Vlans:  Default accounting video sales
BridgeID      80:00:00:e0:2b:00:a4:00
Designated root:  00:00:00:00:00:00:00:00
RootPathCost:  0
MaxAge: 0s      HelloTime: 0s      ForwardDelay: 0s
CfgBrMaxAge: 20s  CfgBrHelloTime: 2s  CfgBrForwardDelay:15s
Topology Change Time: 35s      Hold time: 1s
Topology Change Detected: FALSE  Topology Change:FALSE
Number of Topology Changes: 0
Time Since Last Topology Change: 0s
```

To display port-specific STP information, use the following command:

```
show stpd <stpd_name> port <portlist>
```

This command displays the following:

- STPD port configuration
- STPD state (root bridge, and so on)
- STPD port state (forwarding, blocking, and so on)

DISABLING AND RESETTNG STP

To disable STP or return STP settings to their defaults, use the commands listed in [Table 7-2](#).

Table 7-2: STP Disable and Reset Commands

Command	Description
delete stpd <stpd_name>	Removes an STPD. An STPD can only be removed if all VLANs have been deleted from it.
disable stpd [<stpd_name> all]	Disables the STP mechanism on a particular STPD, or for all STPDs.
disable stpd port <portlist>	Disables STP on one or more ports. Disabling STP on one or more ports puts those ports in FORWARDING state; all BPDUs received on those ports will be disregarded.
unconfig stpd {<stpd_name> all}	Restores default STP values to a particular STPD or to all STPDs.

8

Quality of Service (QoS)

This chapter describes the concept of Quality of Service (QoS) and explains how to implement QoS on the Summit.

OVERVIEW OF QUALITY OF SERVICE

QoS is a feature of the Summit that allows you to specify different service levels for outbound traffic. QoS is an effective control mechanism for networks that have heterogeneous traffic patterns. Using QoS, you can specify the service that a traffic type receives.

The main benefit of QoS is that it allows you to have control over the types of traffic that receive priority service from the Switch. For example, if video traffic requires a higher priority than data traffic, using QoS you can assign a different QoS profile to those VLANs that are transmitting video traffic.

BUILDING BLOCKS

Quality of Service is determined by one or more of the following building blocks:

- **QoS mode** — Indicates whether the Switch should use implicit or explicit traffic classifications. Implicit is the default.
- **QoS profile** — Includes bandwidth and priority parameters.
- **Traffic classification** — Fall into two major groups, those defined implicitly by virtue of their association and those containing some explicit QoS information.

QoS Mode

The QoS mode for the Switch determines with which types of traffic classifications the Switch will be dealing, *explicit* or *implicit*. The default is implicit. If you want to change the QoS mode, it requires performing the change, saving the configuration, and rebooting the Switch.

In the explicit mode, the selection of QoS profiles is fixed and cannot be modified because it is based only on priority. In the implicit mode, QoS profiles, in addition to a single profile that is provided, may be created and include the capability to adjust bandwidth parameters.

QoS Profiles

Depending upon the QoS mode chosen, QoS profiles can be fixed (as with explicit mode) or can be created (as with implicit mode) and contain bandwidth and priority parameters. Unless otherwise noted, a QoS profile can then be assigned to a specific traffic classification (such as a port or VLAN). If a QoS profile is assigned to multiple traffic classifications, those classifications share the same Quality of Service if the traffic shares the same physical ports.

The parameters that make up a QoS profile include the following:

- **Minimum bandwidth** — The minimum percentage of bandwidth that this queue requires. The Switch is required to provide the minimum amount of bandwidth to the queue. The lowest possible value is 0%.
- **Maximum bandwidth** — The maximum percentage of bandwidth that this queue is permitted to use.
- **Priority** — The level of priority in which this queue will be serviced by the Switch. Choices include:
 - Low
 - Normal
 - Medium
 - High

A QoS profile does not alter the behavior of the Switch until it is assigned to a traffic classification.

PREDEFINED QoS PROFILES

The following predefined QoS profiles are provided, depending upon the QoS configuration of the Switch:

- **Implicit QoS Mode** — A single QoS mode, called *besteffort*, is provided. It allows for 0% minimum and 100% maximum bandwidth along with a low-priority setting. Up to 15 other QoS profiles may be defined.
- **Explicit QoS Mode** — Four separate explicit QoS profiles, each with varying priorities, are defined. They are as follows:
 - *qplow*
 - *qpnormal*
 - *qpmedium*
 - *qphigh*

All have bandwidth parameters of a minimum of 10% and a maximum of 100% bandwidth.

CREATING A QoS PROFILE

Up to 32 QoS profiles can be created on the Summit. To create a QoS profile, use the following command:

```
create qosprofile <name>
```

A new QoS profile is created with the following default values:

- Minimum bandwidth — 0%
- Maximum bandwidth — 100%
- Priority — low

Each of the default values is configurable by using the following command:

```
config qosprofile <qosname> {minbw <percent>} {maxbw <percent>}  
{priority <level>}
```

EXPLICIT TRAFFIC CLASSIFICATION

Examples of traffic that have an explicit classification include tagged 802.1Q traffic that contains the defined 802.1p priority bits and other similar mechanisms (such as 3Com's PACE™). It can also be made explicit by virtue of which port in the Switch the traffic was sourced from. Explicitly defined traffic uses only priority in differentiating its QoS. Priority is used when there is bandwidth contention for the Switch to transmit.

PRIORITY MAPPINGS FOR EXPLICIT TRAFFIC

For explicit traffic classification, priority is determined in the following ways:

- Source port — You can assign a source port to one of the four available explicit QoS profiles.
- .1p priority bits — A fixed mapping of the eight possible .1p values is done to the four QoS profile priority categories. Values 0-1 is 'qplow'; 2-3 is 'qpnormal'; 4-5 is 'qpmedium' and 6-7 is 'qphigh'.
- PACE — Traffic with the Universally/Locally (U/L) Administered bit enabled in the source address will be associated with the qpmedium QoS profile.

ASSIGNING A QoS PROFILE TO A TRAFFIC CLASSIFICATION

Once you have established one or more traffic classifications and configured one or more QoS profiles, you must match them together using one of the following commands:

```
config VLAN <name> <portlist> qosprofile <qosname>
```

or

```
config port <portlist> qosprofile <qosname>
```

CONFIGURING QoS

Table 8-1 describes the commands used to configure QoS.

Table 8-1: QoS Configuration Commands

Command	Description
create qosprofile <qosname>	Creates a QoS profile. The default values assigned to a created QoS profile are: <ul style="list-style-type: none">■ Minimum bandwidth — 0%■ Maximum bandwidth — 100%■ Priority — low
config qosmode [explicit implicit]	Changes the QoS mode to explicit mode or implicit mode.
config qosprofile <qosname> {minbw <percent>} {maxbw <percent>} {priority <level>}	Configures a QoS profile. Specify: <ul style="list-style-type: none">■ minbw — The minimum bandwidth percentage guaranteed to be available to this queue. The default setting is 0.■ maxbw — The maximum bandwidth percentage this queue is permitted to use. The default setting is 100.■ priority — The service priority for this queue. Settings include low, medium-low, medium, high. The default setting is low.
config port <portlist> qosprofile <qosname>	Allows you to configure one or more ports to use a particular QoS profile.
config vlan <name> qosprofile <qosname>	Allows you to configure a VLAN to use a particular QoS profile.

SAMPLE QoS CONFIGURATIONS

The following example creates a QoS profile called *fast*. It configures the QoS profile *guarantee* to use a minimum bandwidth percentage of 15%, a maximum bandwidth percentage of 100%, and it assigns the priority level of highest. It configures ports 12 through 16 in the VLAN named *engineering* to use the QoS profile named *guarantee*.

```
create qosprofile guarantee
config qosprofile guarantee minbw 15 maxbw 100 priority highest
config engineering 12-16 qosprofile guarantee
```

DISPLAYING QoS INFORMATION

To display QoS information on the Switch, use the following command:

```
show qosprofile {<qosname> | all}
```

Information displayed includes:

- QoS profile name
- Minimum bandwidth
- Maximum bandwidth
- Priority

RESETTING QoS

To delete a QoS profile use the following command:

```
delete qosprofile <qosname>
```

9

IP Unicast Routing

The chapter describes how to configure IP routing on the Summit. It assumes that you are already familiar with IP unicast routing. If not, refer to the following publications for additional information:

- RFC 1058 — *Routing Information Protocol*
- RFC 1256 — *ICMP Router Discovery Messages*
- RFC 1723 — *RIP Version 2*
- RFC 1812 — *Requirements for IP Version 4 Routers*

OVERVIEW OF IP UNICAST ROUTING

The Summit provides full Layer 3, IP unicast routing. It exchanges routing information with other routers on the network using the Routing Information Protocol (RIP). The Summit dynamically builds and maintains a routing table, and determines the best path for each of its routes.

Each host using the IP unicast routing functionality of the Summit must have a unique IP address assigned. In addition, the default gateway assigned to the host must be the IP address of the Summit router interface.

ROUTER INTERFACES

The routing software and hardware routes IP traffic between router interfaces. A router interface is simply a VLAN that has an IP address assigned to it.

As you create VLANs with IP addresses belonging to different IP subnets, you can also choose to route between the VLANs. Both the VLAN switching and IP routing function occur within the Summit.

In [Figure 9-1](#), A Summit is depicted with two VLANs defined; *Finance* and *Personnel*. Ports 1 and 3 are assigned to *Finance*; ports 2 and 4 are assigned to *Personnel*. *Finance* belongs to the IP network 192.207.35.0; the router interface for *Finance* is assigned the IP address 192.207.35.1. *Personnel* belongs to the IP network 192.207.36.0; its router interface is assigned IP address 192.207.36.1. Traffic within each VLAN is switched using the Ethernet MAC addresses. Traffic between the two VLANs is routed using the IP addresses.

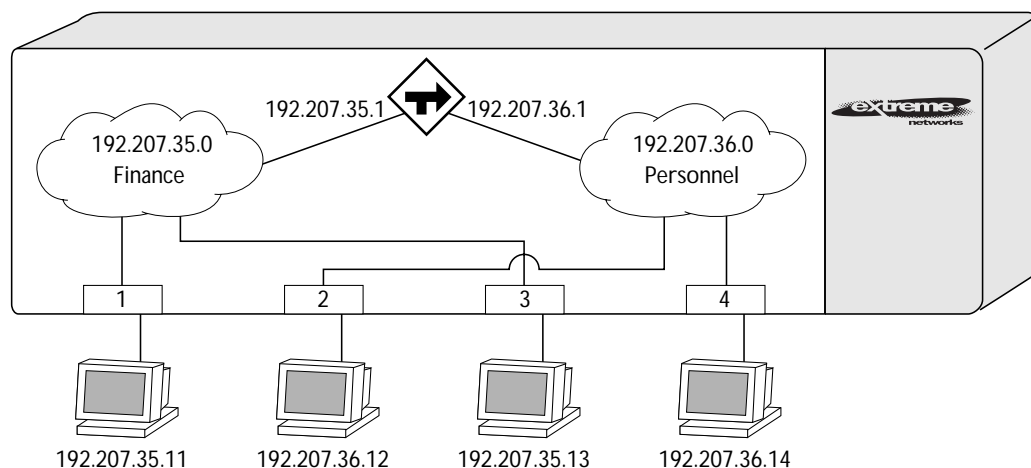


Figure 9-1: Routing between VLANs

POPULATING THE ROUTING TABLE

The Summit maintains an IP routing table for both network routes and host routes. The table is populated from the following sources:

- Dynamically, by way of RIP packets or ICMP redirects exchanged with other routers
- Statically, by way of routes entered by the administrator
 - Default routes, configured by the administrator
 - Locally, by way of interface addresses assigned to the Summit
 - By other static routes, as configured by the administrator

DYNAMIC ROUTES

Dynamic routes are typically learned by way of RIP. Routers that use RIP exchange information in their routing tables in the form of RIP advertisements. Using dynamic routes, the routing table contains only networks that are reachable.

Dynamic routes are aged out of the table when a RIP update for the network is not received for a period of time.

STATIC ROUTES

Static routes are manually entered into the routing table. Static routes are used to reach networks not advertised by routers. You can configure up to 64 static unicast routes on the Summit.

Static routes can also be used for security reasons, to control which routes you want advertised by the router. You can decide if you want all static routes to be advertised, using the following command:

```
[enable | disable] rip exportstatic
```

The default setting is enabled. Static routes are never aged out of the routing table.

MULTIPLE ROUTES

When there are multiple, conflicting choices of a route to a particular destination, the router picks the route with the longest matching network mask. If these are still equal, the router picks the route using the following criterion (in the order specified):

- Directly attached network interfaces
- ICMP redirects (refer to [Table 9-4](#))
- Static routes
- RIP
- Directly attached network interfaces that are not active.

You can also configure *black-hole* routes—traffic to these destinations is silently dropped.

CONFIGURING IP UNICAST ROUTING

This section describes the commands associated with configuring IP unicast routing on the Summit. Configuring routing involves the following steps:

- Verify the Switch operating mode is set to `iprouting`, by using the following command:

```
show switch
```

If it is not, use the following command:

```
config devicemode iprouting
```

- Create and configure two or more VLANs.

For information on creating and configuring VLANs, refer to [Chapter 5](#).

- Assign each VLAN that will be using routing an IP address, using the following command:

```
config vlan <name> ipaddress <ipaddress> {<mask>}
```

Ensure that each VLAN has a unique IP address.

- Configure a default route, using the following command:

```
config iproute add default <gateway> {<metric>}
```

Default routes are used when the router has no other dynamic or static route to the requested destination.

- Turn on IP routing for one or more VLANs, using the following command:

```
enable ipforwarding {vlan <name> | all}
```

- Turn on RIP, using the following command:

```
enable rip
```

When you create a VLAN, RIP is enabled by default. You must, however, enable RIP on the Switch in order to route traffic. To disable RIP on a particular VLAN, use the following command:

```
- config rip delete {vlan <name>}
```


[Table 9-1](#) describes the commands used to configure basic IP settings on the Switch.

Table 9-1: Basic IP Commands

Command	Description
enable bootp {vlan <name> all}	Enables the generation and processing of BOOTP packets on a VLAN to obtain an IP address for the VLAN from a BOOTP server. The default setting is enabled for all VLANs.
enable bootprelay	Enables the forwarding of BOOTP and Dynamic Host Configuration Protocol (DHCP) requests.
enable ipforwarding {vlan <name> all}	Enables IP routing for one or more VLANs. If no argument is provided, enables routing for all VLANs that have been configured with an IP address. The default setting for <code>ipforwarding</code> is disabled.
enable ipforwarding broadcast {vlan <name> all}	Enables forwarding IP broadcast traffic for one or more VLANs. If no argument is provided, enables broadcast forwarding for all VLANs. To enable, <code>ipforwarding</code> must be enabled on the VLAN. The default setting is enabled.
config bootprelay add <ipaddress>	Adds the IP destination address to forward BOOTP packets.
config bootprelay delete [<ipaddress> all]	Removes one or all IP destination addresses for forwarding BOOTP packets.
config iparp add <ipaddress> <mac_address>	Adds a permanent entry to the ARP table. Specify the IP address and MAC address of the entry.
config iparp delete <ipaddress>	Deletes an entry from the ARP table. Specify the IP address of the entry.
disable bootp vlan [<name> all]	Disables the generation and processing of BOOTP packets.
disable bootprelay	Disables the forwarding of BOOTP requests.
disable ipforwarding {vlan <name> all}	Disables routing for one or more VLANs.
disable ipforwarding broadcast {vlan <name> all}	Disables routing of broadcasts to other networks.

Table 9-1: Basic IP Commands (continued)

Command	Description
clear iparp [<ipaddress> vlan <name> all]	Removes dynamic entries in the IP ARP table. Permanent IP ARP entries are not affected.
clear ipfdb [<ipaddress> vlan <name> all]	Removes the dynamic entries in the IP forwarding database.

[Table 9-2](#) describes the commands used to configure the IP route table.

Table 9-2: Route Table Configuration Commands

Command	Description
config iproute add <ipaddress> <mask> <gateway> {<metric>}	Adds a static address to the routing table. Use a value of 255.255.255.255 for <code>mask</code> to indicate a host entry
config iproute delete <ipaddress> <mask> <gateway>	Deletes a static address from the routing table.
config iproute add blackhole <ipaddress> <mask>	Adds a <code>blackhole</code> address to the routing table. All traffic destined for the configured IP address is dropped, and no Internet Control Message Protocol (ICMP) message is generated.
config iproute delete blackhole <ipaddress> <mask>	Deletes a <code>blackhole</code> address from the routing table.
config iproute add default <gateway> {<metric>}	Adds a default gateway to the routing table. A default gateway must be located on a configured IP interface . If no metric is specified, the default metric of 1 is used.
config iproute delete default <gateway>	Deletes a default gateway from the routing table.

Table 9-3 describes the commands used to configure RIP.

Table 9-3: RIP Configuration Commands

Command	Description
enable rip	Enables RIP. The default setting is disabled.
enable rip aggregation	Enables RIP aggregation of subnet information on a RIP version 2 interface. The default setting is enabled.
enable rip exportstatic	Enables the advertisement of static routes using RIP. The default setting is enabled.
enable rippoisonreverse	Enables the split horizon with poison-reverse algorithm for RIP. The default setting is enabled.
enable rip splithorizon	Enables the split horizon algorithm for RIP. Default setting is enabled.
enable rip triggerupdate	Enables triggered updates. <i>Triggered updates</i> are a mechanism for immediately notifying a router's neighbors when the router adds or deletes routes, or changes the metric of a route. The default setting is enabled.
config rip add {vlan <name> all}	Configures RIP on an IP interface. If no VLAN is specified, then <code>all</code> is assumed. When an IP interface is created, per interface RIP configuration is enabled by default.
config rip delete {vlan <name> all}	Disables RIP on an IP interface. When RIP is disabled on the interface, the parameters are not reset to their defaults.
config rip garbage-time {<delay>}	Configures the RIP garbage time. The default setting is 120 seconds.
config rip route-timeout {<delay>}	Configures the route timeout. The default setting is 180 seconds.

Table 9-3: RIP Configuration Commands (continued)

Command	Description
config rip rxmode [none v1only v2only any] {vlan <name> all}	<p>Changes the RIP receive mode for one or more VLANs. Specify:</p> <ul style="list-style-type: none"> ■ none — Drop all received RIP packets. ■ v1only — Accept only RIP version 1 format packets. ■ v2only — Accept only RIP version 2 format packets. ■ any — Accept both version 1 and version 2 packets. <p>If no VLAN is specified, the setting is applied to all VLANs. The default setting is any.</p>
config rip txmode [none v1only v1comp v2only] {vlan <name> all}	<p>Changes the RIP transmission mode for one or more VLANs. Specify:</p> <ul style="list-style-type: none"> ■ none — Do not transmit any packets on this interface. ■ v1only — Transmit RIP version 1 format packets to the broadcast address. ■ v1comp — Transmit version 2 format packets to the broadcast address. ■ v2only — Transmit version 2 format packets to the RIP multicast address <p>If no VLAN is specified, the setting is applied to all VLANs. The default setting is v2only.</p>
config rip updatetime {<delay>}	Changes the periodic RIP update timer. The default setting is 30 seconds.
disable rip	Disables RIP.
disable rip aggregation	Disables the RIP aggregation of subnet information on a RIP version 2 interface.
disable rip splithorizon	Disables split horizon.
disable rip poisonreverse	Disables poison reverse.
disable rip triggerupdate	Disables triggered updates
disable rip exportstatic	Disables the filtering of static routes.
unconfig rip {vlan <name> all}	Resets all RIP parameters to the default VLAN. Does not change the enable/disable state of the RIP settings.

Table 9-4 describes the commands used to configure the ICMP protocol.

Table 9-4: ICMP Configuration Commands

Command	Description
enable icmp redirects {vlan <name> all}	Enables generation of ICMP redirect messages on one or more VLANs. The default setting is enabled.
enable icmp unreachable {vlan <name> all}	Enables the generation of ICMP unreachable messages on one or more VLANs. The default setting is enabled.
enable icmp userredirects	Enables the modification of route table information when an ICMP redirect message is received. The default setting is disabled.
enable irdp {vlan <name> all}	Enables the generation of ICMP router advertisement messages on one or more VLANs. The default setting is enabled.
config irdp [multicast broadcast]	Configures the destination address of the router advertisement messages. The default setting is broadcast.
config irdp <mininterval> <maxinterval> <lifetime> <preference>	Configures the router advertisement message timers, using seconds. Specify: <ul style="list-style-type: none"> ■ <code>mininterval</code> — The minimum amount of time between router advertisements. The default setting is 450 seconds. ■ <code>maxinterval</code> — The maximum time between router advertisements. The default setting is 600 seconds. ■ <code>lifetime</code> — The default setting is 1,800 seconds. ■ <code>preference</code>
unconfig icmp	Resets all ICMP settings to the default values.
unconfig irdp	Resets all router advertisement settings to the default values.
disable icmp redirects {vlan <name> all}	Disables the generation of ICMP redirects on one or more VLANs.
disable icmp unreachable	Disables the generation of ICMP unreachable messages on one or more VLANs.
disable icmp userredirects	Disables the changing of routing table information when an ICMP redirect message is received.

Table 9-4: ICMP Configuration Commands (continued)

Command	Description
disable irdp {vlan <name> all}	Disables the generation of router advertisement messages on one or more VLANs.

ROUTING CONFIGURATION EXAMPLE

Figure 9-2 illustrates a Switch that has three VLANs defined as follows:

- *Finance*
 - Protocol-sensitive VLAN using the IP protocol
 - Ports 1 and 3 have been assigned
 - IP address 192.207.35.1
- *Personnel*
 - Protocol-sensitive VLAN using the IP protocol
 - Ports 2 and 4 have been assigned
 - IP address 192.207.36.1
- *MyCompany*
 - Port-based VLAN
 - All ports have been assigned

The stations connected to ports 1 through 4 generate a combination of IP traffic and NetBIOS traffic. The IP traffic is filtered by the protocol-sensitive VLANs. All other traffic is directed to the VLAN *MyCompany*.

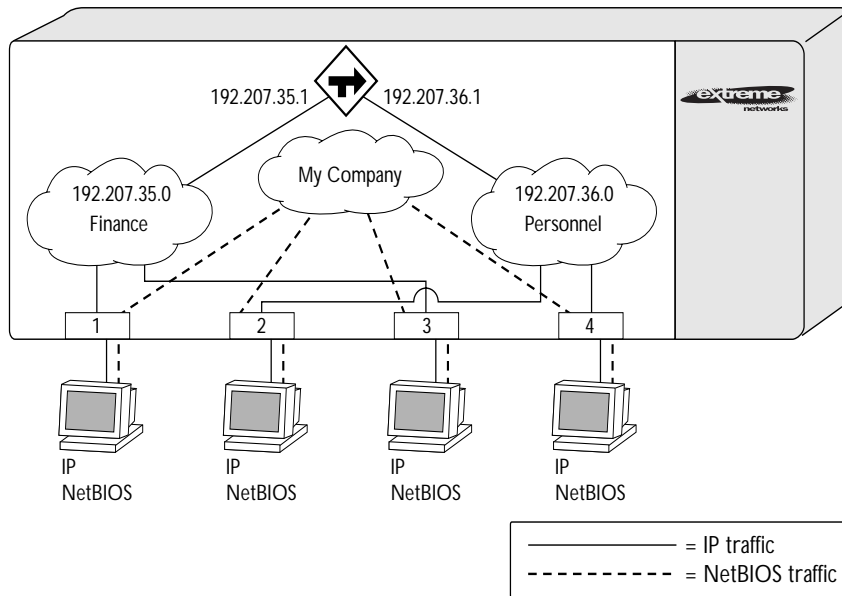


Figure 9-2: Unicast Routing Configuration Example

In this configuration, all IP traffic from stations connected to ports 1 and 3 have access to the router by way of the VLAN *Finance*. Ports 2 and 4 reach the router by way of the VLAN *Personnel*. All other traffic (NetBIOS) is part of the VLAN *MyCompany*.

The example in [Figure 9-2](#) is configured as follows:

```
create vlan Finance
create vlan Personnel
create vlan MyCompany

config Finance protocol ip
config Personnel protocol ip

config Finance add port 1,3
config Personnel add port 2,4
config MyCompany add port all

config Finance ipaddress 192.207.35.1
config Personnel ipaddress 192.207.36.1

enable ipforwarding
enable rip
```

DISPLAYING ROUTER SETTINGS

To display settings for various IP routing components, use the commands listed in [Table 9-5](#).

Table 9-5: Router Show Commands

Command	Description
show ip config {vlan <name> all}	Displays configuration information for one or more VLANs, including the following: <ul style="list-style-type: none">■ IP address, subnet mask■ IP forwarding information■ BOOTP configuration■ VLAN name, VLANid■ Global ICMP configuration■ Global router advertisement configuration
show ip stats {vlan [<name> all]}	Displays IP statistics for the CPU of the Switch.
show iparp {<ipaddress vlan <name> all permanent}	Displays the IP Address Resolution Protocol (ARP) table. You can filter the display by IP address, VLAN, or permanent entries. Each entry displayed includes the following: <ul style="list-style-type: none">■ IP address■ MAC address■ Aging timer value■ VLAN name, VLANid, and port number■ Flags
show ipfdb {<ipaddress> <netmask> vlan <name> all}	Displays the contents of the IP forwarding database table. Used for technical support purposes.
show iproute vlan {<name> all permanent <ipaddress> <netmask>}	Displays the contents of the IP routing table.

Table 9-5: Router Show Commands (continued)

Command	Description
show rip {vlan <name> all}	Displays RIP configuration and statistics for one or more VLANs. Display includes the state for RIP settings, and interface states. Statistics include the following: <ul style="list-style-type: none"> ■ Packets transmitted ■ Packets received ■ Bad packets received ■ Bad routes received ■ Number of RIP peers ■ Peer information
show rip stat {vlan <name> all}	Displays RIP-specific statistics. Statistics include the following per interface: <ul style="list-style-type: none"> ■ Packets transmitted ■ Packets received ■ Bad packets received ■ Bad routes received ■ Number of RIP peers ■ Peer information

RESETTING AND DISABLING ROUTER SETTINGS

To return router settings to their defaults and disable routing functions, use the commands listed in [Table 9-6](#).

Table 9-6: Router Reset and Disable Commands

Command	Description
clear iparp [<ipaddress> vlan <name> all]	Removes dynamic entries in the IP ARP table. Permanent IP ARP entries are not affected.
clear ipfdb [<ipaddress> <netmask> vlan <name> all]	Removes the dynamic entries in the IP forwarding database.
disable bootp vlan [<name> all]	Disables the generation and processing of BOOTP packets.
disable bootprelay	Disables the forwarding of BOOTP requests.

Table 9-6: Router Reset and Disable Commands (continued)

Command	Description
disable icmp redirects {vlan <name> all}	Disables the generation of ICMP redirects on one or more VLANs.
disable icmp unreachable	Disables the generation of ICMP unreachable messages on one or more VLANs.
disable icmp userredirects	Disables the changing of routing table information when an ICMP redirect message is received.
disable ipforwarding {vlan <name> all}	Disables routing for one or more VLANs.
disable ipforwarding broadcast {vlan <name> all}	Disables routing of broadcasts to other networks.
disable irdp {vlan <name> all}	Disables the generation of router advertisement messages on one or more VLANs.
disable rip {vlan <name> all}	Disables RIP for one or more VLANs. When RIP is disabled, the parameters are not reset to their defaults, and the states are not cleared. Disables RIP for a VLAN causes all routes learned from that VLAN to be advertised with a GarbageTime metric of 16, before being deleted from the route table.
disable rip aggregation	Disables the RIP aggregation of subnet information on a RIP version 2 interface.
disable rip splithorizon	Disables split horizon.
disable rip poisonreverse	Disables poison reverse.
disable rip triggerupdate	Disables triggered updates.
disable rip exportstatic	Disables the filtering of static routes.
unconfig icmp	Resets all ICMP settings to the default values.
unconfig irdp	Resets all router advertisement settings to the default values.
unconfig rip {vlan <name> all}	Resets all RIP parameters to the default VLAN. Does not change the enable/disable state of the RIP settings.

10

Status Monitoring and Statistics

This chapter describes how to view the current operating status of the Switch, how to display information in the Switch log, and how to take advantage of the RMON capabilities available in the Switch.

Viewing statistics on a regular basis allows you to see how well your network is performing. If you keep simple daily records, you will see trends emerging and notice problems arising before they cause major network faults. This way, statistics can help you get the best out of your network.

STATUS MONITORING

The status monitoring facility provides information about the Switch. This information may be useful for your technical support representative if you have a problem.

Table 10-1 describes the show commands available on the Switch.

Table 10-1: Switch Monitoring Commands

Command	Description
show account	Displays the account names, access level, number of successful and failed login attempts, and the number of active sessions in the user database. This command is available only to admin level users.
show config	Displays the current Switch configuration to the terminal. You can then capture the output and store it as a file.

Table 10-1: Switch Monitoring Commands (continued)

Command	Description
show fdb {all <macaddress> vlan <name> <portlist> permanent}	Displays the forwarding database contents including MAC address, associated VLAN, port, age-of-entry configuration method, and status. Providing one of the options acts as a filter on the display. Providing a VLAN name displays all entries for the VLAN. Use the MAC address to locate a specific entry in the FDB.
show ip config {vlan <name> all}	Displays configuration information for one or more VLANs, including the following: <ul style="list-style-type: none"> ■ IP address, subnet mask ■ IP forwarding information ■ BOOTP configuration ■ VLAN name, VLANid ■ Global ICMP configuration ■ Global IGMP configuration ■ Global IRDP configuration
show iparp {<ip_address> vlan <name> all permanent}	Displays the current Address Resolution Protocol (ARP) cache for a selected IP address, VLAN, or all entries. With no options, information for all VLANs is displayed. Information displayed includes IP address, MAC address, aging timer value, VLAN name, VLANid, and port number.
show ipfdb {<ipaddress> vlan <name> all}	Displays the contents of the IP forwarding database table. Use for technical support purposes.
show ipmcroute {vlan <name> all permanent}	Displays the contents of the IP multicast route table.
show iproute vlan {<name> all permanent}	Displays the contents of the IP routing table.
show ipstats {vlan [<name> all]}	Displays statistics of packets handled by the CPU, including the following: <ul style="list-style-type: none"> ■ inpackets, outpackets ■ ICMP/IGMP statistics ■ IRDP statistics

Table 10-1: Switch Monitoring Commands (continued)

Command	Description
show log {<priority>} {<subsystem>}	<p>Displays the current snapshot of the log. Options include:</p> <ul style="list-style-type: none"> ■ priority — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed. ■ subsystem — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.
show log config	Displays the log configuration, including the syslog host IP address, the priority level of messages being logged locally, and the priority level of messages being sent to the syslog host.
show management	Displays network management configuration and statistics including enable/disable states for Telnet and SNMP, SNMP community strings, authorized SNMP station list, SNMP trap receiver list, and login statistics.
show memory	Displays the current system memory information.
show port <portlist> collisions	Displays collision statistics for each port.
show port <portlist> config	Displays state, link status, speed, and autonegotiation setting for each port.
show port <portlist> errors	Displays error information for one or more ports.
show port <portlist> packet	Displays a histogram of packet statistics for one or more ports.
show port <portlist> stats	Displays port information including physical layer configuration and statistics.
show protocol {<protocol>< all}	Displays protocol information including protocol name, protocol fields, and the list of VLANs that use this protocol.
show qosprofile {<qosname> all}	Displays QoS profile information including the QoS profile name, minimum bandwidth, maximum bandwidth, and priority levels. Also displays the groupings to which this QoS profile is applied.

Table 10-1: Switch Monitoring Commands (continued)

Command	Description
show rip {vlan <name> all}	<p>Displays RIP configuration and statistics for one or more VLANs. Display includes the state for RIP settings, and interface states. Statistics include the following:</p> <ul style="list-style-type: none"> ■ Packets transmitted ■ Packets received ■ Bad packets received ■ Bad routes received ■ Number of RIP peers ■ Peer information
show rip stat {vlan <name> all}	<p>Displays RIP-specific statistics. Statistics include the following per interface:</p> <ul style="list-style-type: none"> ■ Packets transmitted ■ Packets received ■ Bad packets received ■ Bad routes received ■ Number of RIP peers ■ Peer information
show session	<p>Displays the currently active Telnet and console sessions communicating with the Switch. Provides the user name, IP address of the incoming Telnet session, whether a console session is currently active, and login time. Sessions are numbered.</p>
show stpd {<stpd_name> all}	<p>Displays STP information for the one or all STP domains.</p>
show stpd <stpd_name> port <portlist>	<p>Displays port-specific STP information including STP port configuration and state.</p>

Table 10-1: Switch Monitoring Commands (continued)

Command	Description
show switch	<p>Displays the current Switch information, including:</p> <ul style="list-style-type: none"> ■ sysName, sysLocation, sysContact ■ MAC address ■ Current time and time, and system uptime ■ Operating environment (temperature, fans, and power supply status) ■ NVRAM image information (primary/secondary image, date, time, size, version) ■ NVRAM configuration information (primary/secondary configuration, date, time, size, version) ■ Scheduled reboot information ■ 802.1p information ■ System serial number and reworks indicator ■ Software platform ■ System ID ■ Power supply and fan status
show version	<p>Displays the hardware and software versions currently running on the Switch. Also displays the Switch serial number.</p>
show vlan {<name> all}	<p>When used with the keyword <code>all</code>, or with no named VLANs, displays a summary list of VLAN names with a portlist and associated status of each. When used with a named identifier, displays port information including membership list, IP address, tag information.</p>

PORT STATISTICS

The Summit provides a facility for viewing port statistic information. The summary information lists values for the current counter against every port on the Switch, and it is refreshed approximately every two seconds. Values are displayed to nine digits of accuracy.

To view port statistics, enter

```
show port <portlist> stats
```

The following port statistic information is collected by the Switch:

- **Link Status** — The current status of the link. Options are
 - Ready — The port is ready to accept a link.
 - Active — The link is present at this port.
- **Transmit Packet Count (Tx Pkt Count)** — The number of packets that have been successfully transmitted by the port.
- **Transmit Byte Count (Tx Byte Count)** — The total number of data bytes successfully transmitted by the port.
- **Total Collisions** — The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions.
- **Received Packet Count (Rx Pkt Count)** — The total number of good packets that have been received by the port.
- **Received Byte Count (RX Byte Count)** — The total number of bytes that were received by the port, including bad or lost frames. This number includes bytes contained in the Frame Check Sequence (FCS), but excludes bytes in the preamble.
- **Receive Broadcast (RX Bcast)** — The total number of frames received by the port that are addressed to a broadcast address.
- **Receive Multicast (RX Mcast)** — The total number of frames received by the port that are addressed to a multicast address.

PORT ERRORS

The Summit keeps track of errors for each port.

To view port error, enter

```
show port <portlist> errors
```

The following port error information is collected by the Switch:

- **Link Status** — The current status of the link. Options are
 - Ready — The port is ready to accept a link.
 - Active — The link is present at this port.
- **Transmit Collisions (TX Coll)** — The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions.
- **Transmit Late Collisions (TX Late)** — The total number of collisions that have occurred after the port's transmit window has expired.
- **Transmit Deferred Frames (TX Def)** — The total number of frames that were transmitted by the port after the first transmission attempt was deferred by other network traffic.
- **Transmit Frames Lost (TX Lost)** — The total number of frames that were not completely transmitted by the port because of underflow.
- **Transmit Errored Frames (TX Err)** — The total number of frames that were not completely transmitted by the port because of network errors (such as late collisions or excessive collisions).
- **Receive Bad CRC Frames (RX CRC)** — The total number of frames received by the port that were of the correct length, but contained a bad FCS value.
- **Receive Oversize Frames (RX Over)** — The total number of good frames received by the port that were of greater than the supported maximum length of 1,522 bytes.
- **Receive Undersize Frames (RX Under)** — The total number of frames received by the port that were less than 64 bytes long.
- **Receive Jabber Frames (RX Jab)** — The total number of frames received by the port that was of greater than the support maximum length and had a Cyclic Redundancy Check (CRC) error.
- **Receive Alignment Errors (RX Align)** — The total number of frames received by the port that occurs if a frame has a CRC error and does not contain an integral number of octets.

- **Receive Frames Lost (RX Lost)** — The total number of frames received by the port that were lost because of buffer overflow in the Switch.

SWITCH LOGGING

The Summit log tracks all configuration and fault information pertaining to the device. Each entry in the log contains the following information:

- **Timestamp** — The timestamp records the month and day of the event, along with the time (hours, minutes, and seconds) in the form HH:MM:SS. If the event was caused by a user, the user name is also provided.
- **Fault level** — [Table 10-2](#) describes the three levels of importance that the Switch can assign to a fault.

Table 10-2: Fault Levels Assigned by the Switch

Level	Description
Critical	A desired Switch function is inoperable. The Switch may need to be reset.
Warning	A noncritical error that may lead to a function failure.
Informational	Actions and events that are consistent with expected behavior.

- **Subsystem** — The facility refers to the specific functional area of the Switch to which the error refers. [Table 10-3](#) describes the subsystems.

Table 10-3: Fault Log Subsystems

Subsystem	Description
Syst	General system-related information. Examples include memory, power supply, security violations, fan failure, overheat condition, and configuration mode.
STP	STP information. Examples include an STP state change.
Brdg	Bridge-related functionality. Examples include low table space and queue overflow.
SNMP	SNMP information. Examples include community string violations.

Table 10-3: Fault Log Subsystems

Subsystem	Description
Telnet	Information related to Telnet login and configuration performed by way of a Telnet session.
VLAN	VLAN-related configuration information.
Port	Port management-related configuration. Examples include port statistics and errors.

- **Message** — The message contains the log information with text that is specific to the problem.

LOCAL LOGGING

The Switch maintains 1,000 messages in its internal log. You can display a snapshot of the log at any time by using the command

```
show log {<priority>} {<subsystem>}
```

where the following is true:

- **priority** — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed.
- **subsystem** — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.

REAL-TIME DISPLAY

In addition to viewing a snapshot of the Switch log, you can configure the Switch to maintain a running real-time display of log messages on the console. To turn on the log display, enter the following command:

```
enable log display
```

To configure the log display, use the following command:

```
config log display {<priority>} {<subsystem>}
```

If **priority** is not specified, only messages of critical priority are displayed. If the **subsystem** is not specified, all subsystems are displayed.

If you enable the log display on a terminal connected to the console port, your settings will remain in effect even after your console session is ended (unless you explicitly disable the log display).

When using a Telnet connection, if your Telnet session is disconnected (because of the inactivity timer, or for other reasons), the log display is automatically halted. You must restart the log display by using the `enable log display` command.

REMOTE LOGGING

In addition to maintaining an internal log, the Summit supports remote logging by way of the UNIX Syslog host facility. To enable remote logging, do the following:

- Configure the Syslog host to accept and log messages.
- Enable remote logging by entering the following command:

```
enable syslog
```

- Configure remote logging by using the following command:

```
config syslog <ipaddress> <facility> {<priority>} {<subsystem>}
```

Specify:

- `ipaddress` — The IP address of the syslog host.
- `facility` — The syslog facility level for local use. Options include `local0` through `local7`.
- `priority` — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, only critical priority messages are sent to the syslog host.
- `subsystem` — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are sent to the syslog host.



Refer to your UNIX documentation for more information about the Syslog host facility.

LOGGING COMMANDS

The commands described in [Table 10-4](#) allow you to configure logging options, reset logging options, display the log, and clear the log.

Table 10-4: Logging Commands

Command	Description
config log display {<priority>} {<subsystem>}	<p>Configures the real-time log display. Options include:</p> <ul style="list-style-type: none"> ■ priority — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed. ■ subsystem — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.
config syslog <ip_address> <facility> {<priority>} {<subsystem>}	<p>Configures the syslog host address and filter messages sent to the syslog host. Options include:</p> <ul style="list-style-type: none"> ■ ipaddress — The IP address of the syslog host. ■ facility — The syslog facility level for local use. ■ priority — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, only critical priority messages and are sent to the syslog host. ■ subsystem — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are sent to the syslog host.
enable log display	Enables the log display.
enable syslog	Enables logging to a remote syslog host.

Table 10-4: Logging Commands (continued)

Command	Description
disable log display	Disables the log display.
disable syslog	Disables logging to a remote syslog host.
show log {<priority>} {<subsystem>}	Displays the current snapshot of the log. Options include: <ul style="list-style-type: none"> ■ priority — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, warning, and informational. If not specified, informational priority messages and higher are displayed. ■ subsystem — Filters the log to display messages associated with the selected Switch subsystem. Subsystems include Syst, STP Brdg, SNMP, Telnet, VLAN, and Port. If not specified, all subsystems are displayed.
show log config	Allow you to display the log configuration, including the syslog host IP address, the priority level of messages being logged locally, and the priority level of messages being sent to the syslog host.
clear counters	Allows you to clear all statistics Switch and port counters.
clear log	Allows you to clear the log.

RMON

Using the Remote Monitoring (RMON) capabilities of the Switch allows network administrators to improve Switch efficiency and reduce the load on the network.

The following sections explain more about the RMON concept and the RMON features supported by the Summit.



You can only use the RMON features of the Switch if you have an RMON management application.

ABOUT RMON

RMON is the common abbreviation for the Remote Monitoring Management Information Base (MIB) system defined by the Internet Engineering Task Force (IETF) documents RFC 1271 and RFC 1757, which allows you to monitor LANs remotely.

A typical RMON setup consists of the following two components:

- **RMON probe** — An intelligent, remotely controlled device or software agent that continually collects statistics about a LAN segment or VLAN. The probe transfers the information to a management workstation on request, or when a predefined threshold is crossed.
- **Management workstation** — Communicates with the RMON probe and collects the statistics from it. The workstation does not have to be on the same network as the probe, and can manage the probe by in-band or out-of-band connections.

RMON FEATURES OF THE SWITCH

The IETF defines nine groups of Ethernet RMON statistics. The Summit supports the following four of these groups:

- Statistics
- History
- Alarms
- Events

This section describes these groups, and discusses how they can be used.

STATISTICS

The RMON Ethernet Statistics group provides traffic and error statistics showing packets, bytes, broadcasts, multicasts, and errors on a LAN segment or VLAN.

Information from the Statistics group is used to detect changes in traffic and error patterns in critical areas of the network.

HISTORY

The History group provides historical views of network performance by taking periodic samples of the counters supplied by the Statistics group. The group features user-defined sample intervals and bucket counters for complete customization of trend analysis.

The group is useful for analysis of traffic patterns and trends on a LAN segment or VLAN, and to establish baseline information indicating normal operating parameters.

ALARMS

The Alarms group provides a versatile, general mechanism for setting threshold and sampling intervals to generate events on any RMON variable. Both rising and falling thresholds are supported, and thresholds can be on the absolute value of a variable or its delta value. In addition, alarm thresholds may be autocalibrated or set manually.

Alarms inform you of a network performance problem and can trigger automated action responses through the Events group.

EVENTS

The Events group creates entries in an event log and/or sends SNMP traps to the management workstation. An event is triggered by an RMON alarm. The action taken can be configured to ignore it, to log the event, to send an SNMP trap to the receivers listed in the trap receiver table, or to both log and send a trap. The RMON traps are defined in RFC 1757 for rising and falling thresholds.

Effective use of the Events group saves you time. Rather than having to watch real-time graphs for important occurrences, you can depend on the Event group for notification. Through the SNMP traps, events can trigger other actions, providing a mechanism for an automated response to certain occurrences.

RMON AND THE SWITCH

RMON requires one probe per LAN segment, and standalone RMON probes have traditionally been expensive. Therefore, Extreme's approach has been to build an inexpensive RMON probe into the agent of each Switch. This allows RMON to be widely deployed around the network without costing more than traditional network management. The Summit accurately maintains RMON statistics at the maximum line rate of all of its ports.

For example, statistics can be related to individual ports. Also, because a probe must be able to see all traffic, a stand-alone probe must be attached to a nonsecure port. Implementing RMON in the Switch means that all ports can have security features enabled.

EVENT ACTIONS

The actions that you can define for each alarm are shown in ..

Table 10-5: Event Actions

Action	High Threshold
No action	
Notify only	Send trap to all trap receivers.
Notify and log	Send trap; place entry in RMON log

11

Software Upgrade and Boot Options

This chapter describes the procedure for upgrading the Switch software image. This chapter also discusses how to save and load a primary and secondary image and configuration file on the Switch.

USING TFTP TO DOWNLOAD A NEW IMAGE

The image file contains the executable code that runs on the Summit. It comes preinstalled on the Switch from the factory. As new versions of the image are released, you should upgrade the software running on your Switch.

The image is upgraded by using a download procedure from a TFTP server on the network. Downloading a new image involves the following steps:

- Load the new image onto a TFTP server on your network.
- Download the new image to the Summit using the following command:

```
download image <ipaddress> <filename> {primary | secondary}
```

where:

- `ipaddress` — is the IP address of the TFTP server.
- `filename` — is the filename of the new image.
- `primary` — indicates the primary image.
- `secondary` — indicates the secondary image.

The Summit can store up to two images: a primary and a secondary. When you download a new image, you must select into which image space (primary or secondary) you want the new image to be placed.

You can select which image the Switch will load on the next reboot by using the following command:

```
use image {primary | secondary}
```

If you do not specify which image to use, the Switch automatically loads the primary image.

REBOOTING THE SWITCH

To reboot the Switch, use the command

```
reboot {<time>}
```

where `time` is the date and time (using a 24-hour clock format) when the Switch will be rebooted. The values use the following format:

```
mm/dd/yyyy hh:mm:ss
```

If you do not specify a reboot time, the reboot will happen immediately following the command.

SAVING CONFIGURATION CHANGES

The configuration is the customized set of parameters that you have selected to run on the Switch. As you make configuration changes, the new settings are stored in run-time memory. Settings that are stored in run-time memory are not retained by the Switch when the Switch is rebooted. To retain the settings, and have them be loaded when you reboot the Switch, you must save the configuration to nonvolatile RAM (NVRAM).

The Summit can store two different configurations: a primary and a secondary. When you save configuration changes, you can select to which configuration you want the changes saved. If you do not specify, the changes are saved to the configuration area current in use.

If you have made a mistake, or you must revert to the configuration as it was before you started making changes, you can tell the Switch to use the secondary configuration on the next reboot.

To save the configuration, use the following command:

```
save {config} {primary | secondary}
```

To use the configuration, use the following command:

```
use config {primary | secondary}
```

The configuration takes effect on the next reboot.

RETURNING TO FACTORY DEFAULTS

To return the Switch configuration to factory defaults, enter the following command:

```
unconfig switch
```

This command resets the entire configuration, with the exception of user accounts and passwords that have been configured.

To reset all parameters, enter the following command:

```
unconfig switch all
```

BOOT OPTION COMMANDS

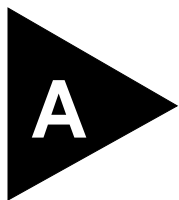
[Table 11-1](#) lists the commands associated with Summit boot options.

Table 11-1: Boot Option Commands

Command	Description
download config <ipaddress> <filename>	Downloads a previously saved ASCII configuration file from a specific IP host. You must specify the IP address of the host and the configuration filename.
download image <ipaddress> <filename> {primary secondary}	Downloads a new image from a TFTP server. You must specify the IP address of the TFTP server and the image filename.
save {config} {primary secondary}	Saves the current configuration of the Switch to NVRAM. You can specify the primary or secondary configuration area. If not specified, the configuration is saved to the configuration area currently in use.

Table 11-1: Boot Option Commands (continued)

Command	Description
use config {primary secondary }	Configures the Switch to use a particular configuration on the next reboot. Options include the primary configuration area, or the secondary configuration area. If not specified, the Switch will use the primary configuration area.
use image {primary secondary}	Configures the Switch to use a particular image on the next reboot. If not specified, the Switch uses the primary image.



Safety Information

IMPORTANT SAFETY INFORMATION



Please read the following safety information thoroughly before installing the Summit Switch.

- Installation and removal of the unit must be carried out by qualified personnel only.
- To reduce the risk of fire or electrical shock, install the unit in a temperature- and humidity-controlled indoor area free of conductive contaminants.

POWER

- Disconnect power from the unit before removing the cover of the unit.
- To ensure compliance with international safety standards, only use the power adapter that is supplied with the unit.
- Disconnect the power adapter before removing the unit.
- The unit must be grounded.
- The unit must be connected to a grounded outlet to comply with European safety standards.
- Do not connect the unit to an A C outlet (power supply) without a ground connection.
- The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.

- This unit operates under Safety Extra Low Voltage (SELV) conditions according to IEC 950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.
- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN60320/IEC320 appliance inlet.
- *France and Peru only*
This unit cannot be powered from IT+ supplies. If your supplies are of IT type, this unit must be powered by 230V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labeled Neutral, connected directly to ground.

POWER CORD

- This must be approved for the country where it is used:

USA and
Canada


- The cord set must be UL-approved and CSA-certified.
- The minimum specification for the flexible cord is No. 18 AWG, Type SV or SJ, 3-conductor.
- The cord set must have a rated current capacity of at least 10A.
- The attachment plug must be an earth-grounding type with a NEMA 5-15P (15A, 125V) or NEMA 6-15P (15A, 250V) configuration.

Denmark

- The supply plug must comply with section 107-2-D1, standard DK2-1a or DK2-5a.

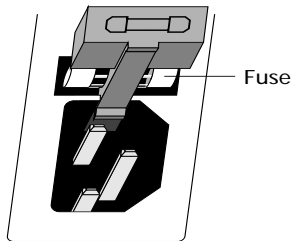
Switzerland

- The supply plug must comply with SEV/ASE 1011.

- If the power cord plug is unsuitable and must be replaced, you may find other codings for the respective connections. Connect the power supply wires for the unit according to the following scheme:
 - Brown wire to the Live (Line) plug terminal, which may be marked with the letter “L” or colored red.
 - Blue wire to the Neutral plug terminal, which may be marked with the letter “N” or colored black.
 - Yellow/Green wire to the Ground plug terminal, which may be marked with the letter “E” or the Earth symbol  or colored yellow/green.

FUSE

- Disconnect power from the unit before opening the fuse holder cover. The unit automatically adjusts to the supply voltage. The fuse is suitable for both 110V A.C. and 220-240V A.C. operation.
To change the fuse, release the fuse holder by gently levering a small screwdriver under the fuse holder catch. Only fuses of the same manufacturer, rating, and type as the original must be used with the unit. Close the fuse holder.



- To comply with European safety standards, a spare fuse must not be fitted to the appliance inlet. Only fuses of the same manufacturer, make, and type must be used with the unit.

CONNECTIONS

- **Fiber Optic ports - Optical Safety.** Never look at the transmit LED/laser through a magnifying device while it is powered on. Never look directly at the fiber TX port and fiber cable ends when they are powered on.
- CLASS 1 LASER DEVICE

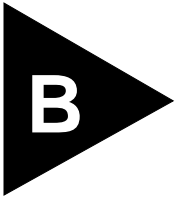
LITHIUM BATTERY

- Replace the lithium battery with the same or equivalent type, as recommended by the manufacturer.




There is a danger of explosion if the battery is incorrectly replaced.

- Dispose of used batteries according to the manufacturer's instructions.
 - Do not dispose of the batteries in water, or by fire.
 - Disposal requirements vary by country and by state.
 - Lithium batteries are not listed by the Environmental Protection Agency (EPA) as a hazardous waste. Therefore, they can typically be disposed of as normal waste.
 - If you are disposing of large quantities, contact a local waste-management service.
- No hazardous compounds are used within the battery module.
- The weight of the lithium contained in each coin cell is approximately 0.035 grams.
- Two types of batteries are used interchangeably:
 - CR chemistry uses manganese dioxide as the cathode material.
 - BR chemistry uses poly-carbonmonofluoride as the cathode material.
- The battery in the bq4830 device is encapsulated and not user-replaceable.

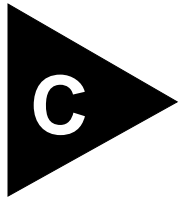


Technical Specifications

Physical Dimensions	Height: 3.5 inches x Width: 17.32 inches x Depth: 17.32 inches Weight: 10 kg
Environmental Requirements	
Operating Temperature	0 to 40° C
Storage Temperature	-10 to 70° C
Operating Humidity	10% to 95% relative humidity, noncondensing
Standards	EN60068 (IEC68)
Safety	
Agency Certifications	UL 1950 3rd Edition, listed cUL listed to CSA 22.2#950 TUV GS mark & GOST safety approval to the following EN standards: <ul style="list-style-type: none">■ EN60960:1992/A3:1995 plus ZB/ZC Deviations■ EN60825-1
Electromagnetic Compatibility	FCC part 15 Class A CSA C108.8-M11983 (A) VCCI Class 2 EN55022 Class B; Summit2: EN55022 Class A EN50082 -1 (1997) C-Tick mark to AS/NZS 3548:1995
	<i>The Summit2 is a Class A product. In a domestic environment, this product may cause radio interference. If this is the case, you may be required to take adequate measures.</i>

Heat Dissipation	118W maximum (341.2 BTU/hr maximum)
Power Supply	
AC Line Frequency	47Hz to 63Hz
Input Voltage Options	90VAC to 264VAC, auto-ranging
Current Rating	100-120/200-240 VAC 3.0/1.5 A

Standards Supported	SNMP SNMP protocol (RFC 1157) MIB-II (RFC 1213) Bridge MIB (RFC 1493) VLAN MIB (RFC 1573) RMON MIB (RFC 1757) Terminal Emulation Telnet (RFC 854)	Protocols Used for Administration UDP (RFC 768) IP (RFC 791) ICMP (RFC 792) TCP (RFC 793) ARP (RFC 826) TFTP (RFC 783) BOOTP (RFC 1271)
---------------------	--	---



Troubleshooting

If you encounter problems when using the Switch, this appendix may be helpful. If you have a problem not listed here or in the release notes, contact your local technical support representative.

LEDs

Power LED does not light:

Check that the power cable is firmly connected to the device and to the supply outlet.

Check the unit fuse. For information on changing the fuse, see [Appendix A](#).

On powering-up, the MGMT LED lights yellow:

The device has failed its Power On Self Test (POST) and you should contact your supplier for advice.

A link is connected, but the Status LED does not light:

Check that:

- All connections are secure.
- Cables are free from damage.
- The devices at both ends of the link are powered-up.
- Both ends of the gigabit link are set to the same autonegotiation state.

Both sides of the gigabit link must be enabled or disabled. If the two are different, typically the side with autonegotiation disabled will have the link LED list, and the side with autonegotiation enabled will not list. The default configuration for a gigabit port is autonegotiation enabled. This can be verified by entering the following command:

```
show port config
```

USING THE COMMAND-LINE INTERFACE

The initial welcome prompt does not display:

Check that your terminal or terminal emulator is correctly configured.

For console port access, you may need to press [Return] several times before the welcome prompt appears.

Check the settings on your terminal or terminal emulator. The settings are 9600 baud, 8 data bits, 1 stop bit, no parity, XON/OFF flow control enabled.

The SNMP Network Manager cannot access the device:

Check that the device's IP address, subnet mask, and default router are correctly configured, and that the device has been reset.

Check that the device's IP address is correctly recorded by the SNMP Network Manager (refer to the user documentation for the Network Manager).

Check that the community strings configured for the Switch and Network Manager are the same.

Check that SNMP access was not disabled for the Switch.

The Telnet workstation cannot access the device:

Check that the device's IP address, subnet mask and default router are correctly configured, and that the device has been reset. Ensure that you enter the IP address of the Switch correctly when invoking the Telnet facility. Check that Telnet access was not disabled for the Switch. If you attempt to log in and the maximum number of Telnet sessions are being used, you should receive an error message indicating so.

Traps are not received by the SNMP Network Manager:

Check that the SNMP Network Manager's IP address and community string are correctly configured, and that the IP address of the Trap Receiver is configured properly on the Switch.

The SNMP Network Manager or Telnet workstation can no longer access the device:

Check that Telnet access or SNMP access is enabled.

Check that the port through which you are trying to access the device has not been disabled. If it is enabled, check the connections and network cabling at the port.

Check that the port through which you are trying to access the device is in a correctly configured VLAN.

Try accessing the device through a different port. If you can now access the device, a problem with the original port is indicated. Re-examine the connections and cabling.

A network problem may be preventing you accessing the device over the network. Try accessing the device through the console port.

Check that the community strings configured for the Switch and the Network Manager are the same.

Check that SNMP access was not disabled for the Switch.

Permanent entries remain in the FDB

If you have made a permanent entry in the FDB (which requires you to specify the VLAN to which it belongs and then delete the VLAN) the FDB entry will remain. Though causing no harm, you must manually delete the entry from the FDB if you want to remove it.

Default and Static Routes

If you have defined static or default routes, those routes will remain in the configuration independent of whether the VLAN and VLAN IP address that used them remains. You should manually delete the routes if no VLAN IP address is capable of using them.

You forget your password and cannot log in:

If you are not an administrator, another user having administrator access level can log in, delete your user name, and create a new user name for you, with a new password.

Alternatively, another user having administrator access level can log in and initialize the device. This will return all configuration information (including passwords) to the initial values.

In the case where no one knows a password for an administrator level user, contact your supplier.

VLANs**You cannot add a port to a VLAN:**

If you attempt to add a port to a VLAN and get an error message similar to

```
localhost:7 # config vlan marketing add port 1,2
ERROR: Protocol conflict.
```

you already have a VLAN using untagged traffic on a port. Only one VLAN using untagged traffic can be configured on a single physical port. VLAN configuration can be verified by using the command

```
show vlan <name>
```

The solution for this error is to remove ports 1 and 2 from the VLAN currently using untagged traffic on those ports. If this were the “default” VLAN, the command would be

```
localhost:23 # config vlan default del port 1,2
```

which should now allow you to re-enter the previous command without error as follows:

```
localhost:26 # config vlan red add port 1,2
```


VLAN names:

There are restrictions on VLAN names. They cannot contain white spaces and cannot start with a numeric value unless you use quotation marks around the name. If a name contains white spaces or starts with a numeric, you must use quotation marks whenever referring to the VLAN name.

802.1Q links do not work correctly:

Remember that VLAN names are only locally significant through the command-line interface. In order for two Switches to communicate across a 802.1Q link, the VLAN ID for the VLAN on one Switch should have a corresponding VLAN ID for the VLAN on the other Switch.

If you are connecting to a third-party device and have checked that the VLAN IDs are the same, the Ethertype field used to identify packets as 802.1Q packets may differ between the devices. The default value used by the Switch is **8100**. If the third-party device differs from this and cannot be changed, you may change the 802.1Q Ethertype used by the Switch with the following command:

```
config dot1p ethertype <ethertype>
```

Changing this parameter changes how the Switch recognizes all tagged frames received, as well as the value it inserts in all tagged frames it transmits.

VLANs, IP Addresses and default routes:

Recall that the Switch can have an IP address for each configured VLAN. It is only necessary to have an IP address associated with a VLAN if you intend to manage (telnet, SNMP, ping) through that VLAN. You can also configure multiple default routes for the Switch. The Switch first tries the default route with the lowest cost metric.

STP**You have connected an endstation directly to the Switch and the endstation fails to boot correctly:**

The Switch has STP enabled, and the endstation is booting before the STP initialization process is complete. Specify that STP has been disabled for that VLAN, or turn off STP for the Switch ports of the endstation and devices it is attempting to connect to, and then reboot the endstation.

The Switch keeps aging out endstation entries in the Switch Forwarding Database (FDB):

Reduce the number of topology changes by disabling STP on those Switches that do not use redundant paths.

Specify that the endstation entries are static or permanent.